KOBIL Smart Token V1.0
User's Guide

January, 27th 2003
English Version

Contents

1 Installation **3**
- 1.1 Package Contents . . . 3
- 1.2 System Requirements . . . 3
- 1.3 Inserting your SIM card into KAAN SIM . . . 4
- 1.4 Installation . . . 5

2 Using KOBIL Smart Token for Microsoft Applications **9**
- 2.1 Certificate Management . . . 9
  - 2.1.1 Getting Your Certificate . . . 9
  - 2.1.2 The Windows Certificate Manager . . . 12
  - 2.1.3 Importing a CA Certificate . . . 13
  - 2.1.4 Importing another User's Certificate . . . 14
- 2.2 Securing Internet Web Access using Internet Explorer . . . 15
- 2.3 Secure E-mail Communication using Microsoft Outlook . . . 18
  - 2.3.1 Choose your Certificate . . . 18
  - 2.3.2 Sending secure E-mail . . . 22
  - 2.3.3 Receiving secure E-mail . . . 23
- 2.4 The Token Manager . . . 26
  - 2.4.1 Delete certificates from your SIM card . . . 27
  - 2.4.2 Import certificates onto your SIM card . . . 27
  - 2.4.3 Changing and Unblocking the SIM card's PIN . . . 27

3 Smart card Logon for Windows 2000/XP **28**
- 3.1 Prerequisites . . . 28
- 3.2 Enrollment Agent Certificate . . . 29
- 3.3 Issuing Smart Card Logon Certificates . . . 32
- 3.4 The Smart Card Logon Process . . . 34
- 3.5 Smartcard-Login in Citrix Metaframe XP Environments . . . 35

4 Using the KOBIL Smart Token PKCS#11 Module for Netscape **36**
- 4.1 Certificate Management with Netscape . . . 36
  - 4.1.1 Getting your Certificate . . . 36
  - 4.1.2 Managing Certificates . . . 39
  - 4.1.3 Importing a new CA Certificate . . . 41
  - 4.1.4 Importing another User's Certificate . . . 41
  - 4.1.5 Importing a Web Server's Certificate . . . 42
  - 4.1.6 Changing the PIN of your SIM card . . . 42
- 4.2 Secure Web Sessions using Netscape Navigator . . . 42
- 4.3 Secure E-mail Communication using Netscape Messenger . . . 43
  - 4.3.1 Choose your Certificate . . . 43
  - 4.3.2 Sending secure E-Mail . . . 45
  - 4.3.3 Receiving secure E-Mail . . . 45

A Problems and Solutions **46**
A.1 KOBIL Smart Token for Microsoft-Applications . . . 46
A.2 KOBIL Smart Token PKCS#11 module for Netscape . . . 47

B Cryptographic Basics and Standards **48**
B.1 Security Objectives . . . 48
B.2 Terms and Basics . . . 48
B.3 Standards . . . 49
B.3.1 Data Digestion Algorithms . . . 49
B.3.2 Symmetric Encryption Algorithms . . . 49
B.3.3 Public Key Algorithms . . . 49
B.3.4 Digital Certificates . . . 52
B.3.5 Certificate Authorities . . . 54
B.3.6 Smart Cards and Readers . . . 55
B.3.7 Secure Socket Layer(SSL) . . . 55
B.3.8 Secure Multipurpose Internet Mail Exchange (S/MIME) . . . 55

C Glossary **59**

Chapter 1

Installation

1.1 Package Contents

- KOBIL USB mini smart card terminal KAAN SIM
- USB cable
- Flyer **Installing KOBIL Smart Token**
- TCOS smart card in SIM format (ID-000)
- CD-ROM with KOBIL Smart Token Software

1.2 System Requirements

- Microsoft Windows XP (at least Service Pack 1) or
  Microsoft Windows 2000 (at least Service Pack 2)
- Microsoft Internet Explorer at least Version 5.5
- Microsoft Office xp or
  Microsoft Outlook 2000 SR-1 or
  Microsoft Outlook Express at least Version 5
- 128 MB RAM
- 10 MB hard disk space
- CD-ROM or DVD-ROM drive
- A free USB-1.1 connector

1.3 Inserting your SIM card into KAAN SIM

Break the SIM card out of the card body by slightly pressing it down.

Open the upper cover of KAAN SIM with a slight pressure to the back. Now, you can insert the SIM card after breaking it out of the card body, facing the contact side down. Figure 1.1 shows how to insert the SIM card.

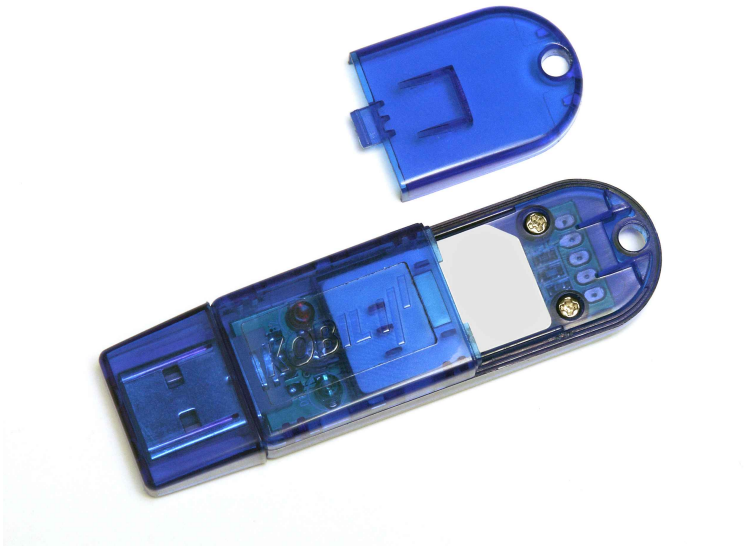

Figure 1.1: Inserting the SIM card into KOBIL Smart Token

Important: The SIM card can remain inside KAAN SIM. You only need to change it if it is broken or if you want to use a new SIM card.

1.4 Installation

Before installing KOBIL Smart Token, please make sure that your Token is not connected to the computer yet. If you have already connected it and the hardware wizard occurs, click on *cancel* to stop the hardware wizard and remove the Token.

1. Quit all running programs
2. Insert your KOBIL Smart Token CD-ROM into your CD-ROM drive. Installation should start automatically. If this is not the case, start it manually by clicking Start - Execute and type **D:\Setup.exe** (replace *D* with your CD-ROM drive's drive letter).

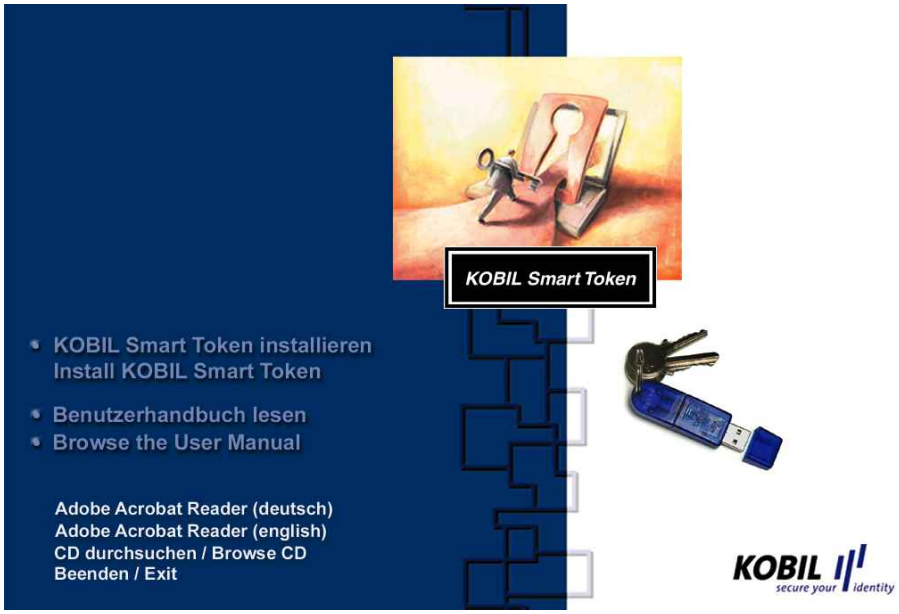

Figure 1.2: KOBIL Smart Token CD-ROM start menu

3. Choose *Install KOBIL Smart Token*.
4. Now, you are asked for your installation language.

Wählen Sie eine Setup-Sprache aus
Wählen Sie die Sprache dieser Installation aus der unten aufgeführten Auswahl aus.
Deutsch
OK
Abbrechen

Figure 1.3: Installation Language

5. You have to agree to the licence agreement to continue installation.

InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
Press the PAGE DOWN key to see the rest of the agreement.
EXPLANATIONS CONCERNING THE RANGE OF THE GRANTED RIGHTS OF USE AND THE WARRANTY AND LIABILITY LIMITATIONS
IMPORTANT - PLEASE READ CAREFULLY
This declaration concerning the range of the granted rights of use and the warranty and liability limitations represents a contractual agreement between you (i.e. either a natural person or a legal entity) and KOBIL Systems GmbH ("KOBIL") concerning the exploitation of the earlier mentioned products according to their provision including the entity of
Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install KOBIL Smart Token, you must accept this agreement.
InstallShield
< Back
Yes
No

Figure 1.4: Licence Agreement

6. Enter the destination path for the KOBIL Smart Token program files. By default, it is **C:\Program Files \KOBIL Systems\KOBIL Smart Token**.

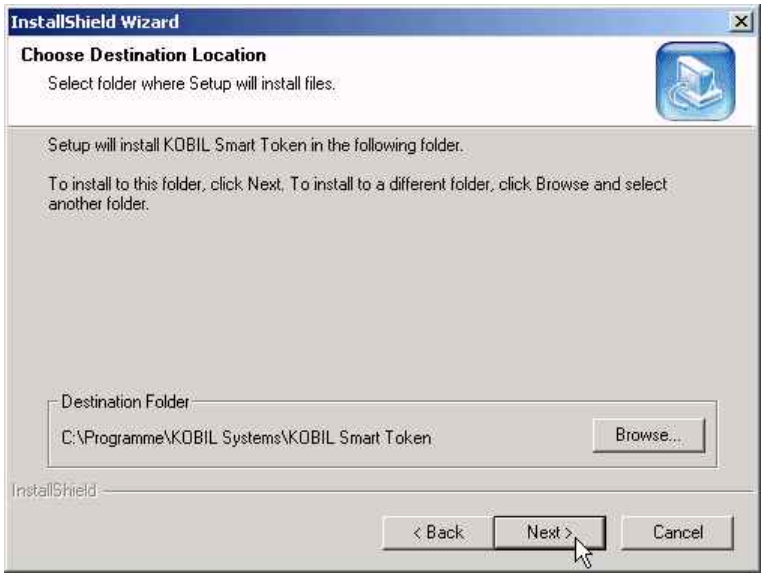
InstallShield Wizard
Choose Destination Location
Select folder where Setup will install files.
Setup will install KOBIL Smart Token in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\Programme\KOBIL Systems\KOBIL Smart Token
Browse...
InstallShield
< Back
Next >
Cancel

Figure 1.5: Installation Path

7. Under some circumstances, it may happen that a warning message appears about the driver's digital signature. You can click on **Yes** (Windows 2000) or **continue anyway** (Windows XP) without concern.

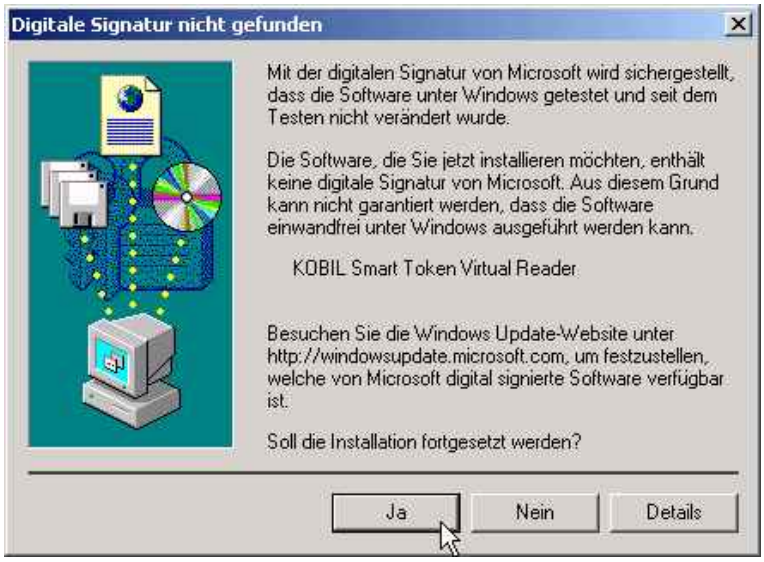
Digitale Signatur nicht gefunden
Mit der digitalen Signatur von Microsoft wird sichergestellt, dass die Software unter Windows getestet und seit dem Testen nicht verändert wurde.
Die Software, die Sie jetzt installieren möchten, enthält keine digitale Signatur von Microsoft. Aus diesem Grund kann nicht garantiert werden, dass die Software einwandfrei unter Windows ausgeführt werden kann.
KOBIL Smart Token Virtual Reader
Besuchen Sie die Windows Update-Website unter http://windowsupdate.microsoft.com, um festzustellen, welche von Microsoft digital signierte Software verfügbar ist.
Soll die Installation fortgesetzt werden?
Ja
Nein
Details

Figure 1.6: Driver's Digital Signature

8. Now, you are asked to insert your KOBIL Smart Token into a free USB port of your computer. If you use a USB hub, please make sure to use a so-called *Powered Hub* which has its own power supply. After inserting KOBIL Smart Token, klick on **OK**.

Figure 1.7: Inserting the Token

9. Now, KOBIL Smart Token installation is completed. Click on **Finish** in the last dialogue box.

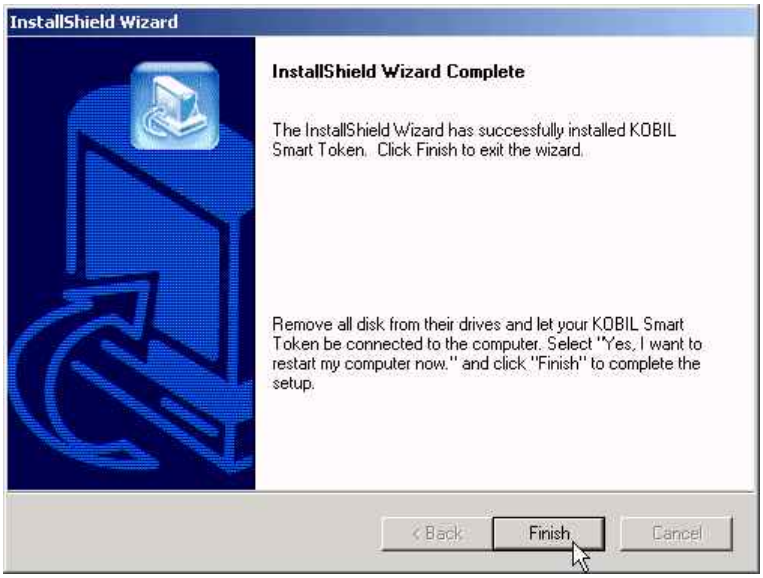
InstallShield Wizard
InstallShield Wizard Complete
The InstallShield Wizard has successfully installed KOBIL Smart Token. Click Finish to exit the wizard.
Remove all disk from their drives and let your KOBIL Smart Token be connected to the computer. Select "Yes, I want to restart my computer now." and click "Finish" to complete the setup.
< Back
Finish
Cancel

Figure 1.8: Abschluss der Installation

Chapter 2

Using KOBIL Smart Token for Microsoft Applications

KOBIL Smart Token for Microsoft applications consists of a so-called *Cryptographic Service Provider* (CSP) for the Microsoft CryptoAPI as well as some tools. This way, all programs compatible with the CryptoAPI – like Internet Explorer or Outlook – work perfectly together with KOBIL Smart Token.

2.1 Certificate Management

KOBIL Smart Token is integrated completely into the Windows certificate management. This chapter therefore explains the usage of the Windows certificate management mechanisms.

First, we must distinguish between two cases:

- **If you have already a personalized SIM card**, you can skip section 2.1.1. This is the case if you get your SIM card from your administrator.
- **If your SIM card is still empty**, continue reading section 2.1.1.

2.1.1 Getting Your Certificate

You'll have to do these steps only if you don't have any certificate on your SIM card yet.

1. Insert your KOBIL Smart Token in your computer's USB port. The SIM card is already inserted into KOBIL Smart Token (see section 1.3)
2. Run Internet Explorer
3. Surf into your preferred Certificate Authority's web page like
   TeleSec-Trustcenter (Germany): www.telesec.de
   TC Trustcenter (Germany): www.trustcenter.de
   Verisign (USA): www.verisign.com
4. Find the page to get a certificate. You may choose to get a demo certificate.

5. Each CA requires similar entries:

   (a) Some basic information such as your name and e-mail address.
   Make sure to spell your e-mail address correctly. If you don't, e-mail signature/encryption will not work!

   (b) A public key algorithm and key size (RSA-1024 is advised).

   (c) A digest algorithm to be used for the creation of certificate's signature (SHA1 is advised).

   (d) A CSP name (**KOBIL Token CSP v1.0** must be selected).

6. Submit your request. At this point, your keys will be generated and written into your SIM card. Your public key and other entries are sent to the CA's server. You have to enter your PIN as shown in figure 2.1 if your SIM card already has a PIN. Otherwise, you are asked to enter your SIM card's PUK and PIN for the first time.

Figure 2.1: PIN entry dialogue

7. You will get your certificate immediately on the next page or it will be sent to you by e-mail.

8. You should install your certificate. Installation procedure should be described in your e-mail or on the current web page. Finally your certificate will be written into your card and it will be registered on that computer.

9. Take a look on your new certificate using the windows certificate manager as described in section 2.1.2. If your certificate is not valid **because of lacking information**, you will have to **import the ca certificate** of your Certificate Authority as described in section 2.1.3.

Contents of Your Digital ID
Fill in all fields. Use only the English alphabet with no accented characters. This information is included in your Digital ID and is available to the public.
First Name:
Nickname or middle initial allowed
(example -- Jack B.)
Last Name:
(example -- Doe)
Your E-mail Address:
(example -- jbdoe@verisign.com)
Choose a Full-service Class 1 Digital ID, or a 60-day Trial Class 1 Digital ID
I'd like a one-year, full-service Digital ID for only US$14.95 per year.
I'd like to test drive a 60-day trial Digital ID for free.
Does not include revocation, replacement, renewal or coverage under the NetSure Protection Plan.
(Optional): Select The Cryptographic Service
If you have a domestic version of this browser you are offered an Enhanced Cryptographic option which provides 1024-bit key encryption. The MS Base Cryptographic provider offers 512-bit key encryption which is adequate for most applications today, but you may select the Enhanced option if your browser offers this choice and you require the higher encryption strength. If you use a specialized mechanism such as a smartcard, please select the appropriate provider as directed by the manufacturer.
Cryptographic Service Provider Name
Kobil Smart CSP v1.0
Digital ID Subscriber Agreement
You must read this subscriber agreement before applying for, accepting, or using a Digital ID (certificate). If you do not agree to the terms of this subscriber agreement, do not apply for, accept, or use the Digital ID (certificate).
THIS SUBSCRIBER AGREEMENT will become effective on the date you submit the certificate application to the designated Issuing Authority (IA). By submitting this Subscriber Agreement (and certificate application) you are requesting that the IA issue a Digital ID (certificate) to you and are expressing your agreement to the terms of this Subscriber Agreement. VeriSign's Public Certification Services are governed by VeriSign's Certification Practice Statement (the "CPS") as amended from time to time, which is incorporated by reference into this Subscriber Agreement. The CPS is published on the Internet in VeriSign's
Read CPS
Download CPS
If you agree to the terms of the Subscriber Agreement, please click ACCEPT to continue.
Accept
Decline

Figure 2.2: The Certificate Request Page of Verisign CA

2.1.2 The Windows Certificate Manager

The Windows Certificate Manager dialogue can be reached by using Internet Explorer or Outlook Express. This dialogue lists all certificates that belong to you (personal), other people, and CAs in separate tabs. You can view and remove any certificates after a selection.

Warning: Be careful with deleting certificates from your KOBIL Smart Token, since afterwards, you will not be able to decrypt any data encrypted with that certificate!

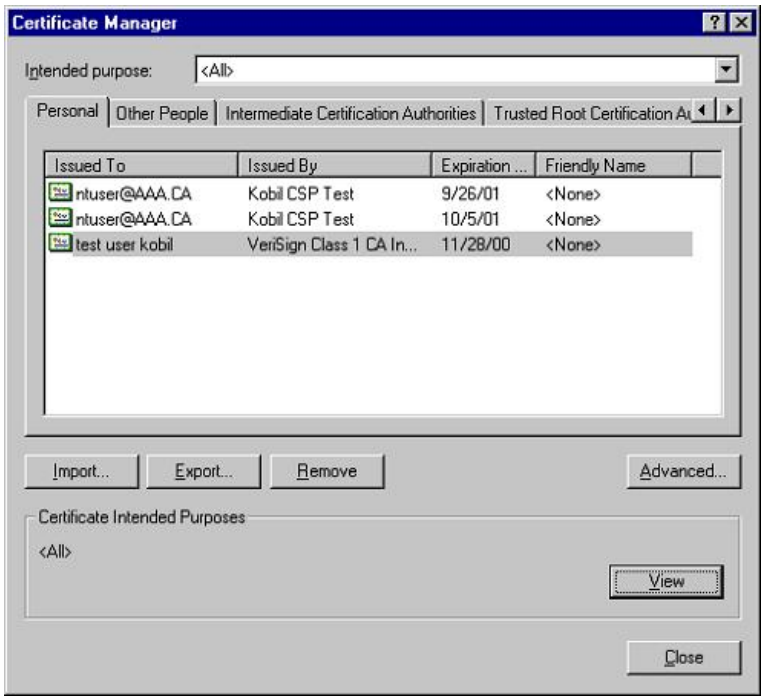

Figure 2.3: The Windows Certificate Manager

To reach the Certificate Manager dialogue from Internet Explorer, click

Tools > Internet Options > Content > Certificates

To reach the Certificate Manager dialog from Outlook Express, click

Tools > Options > Security > Digital IDs

You can see the details and trust path of a certificate from the Certificate dialogue. Trust path includes the root and intermediate CA certificates that sign and approve this certificate in an order. If any of the certificate in the path is not trusted (its signature is not valid or the root CA is unknown), that certificate and all other certificates under it will be marked with a red cross, showing that those certificates can not be used.

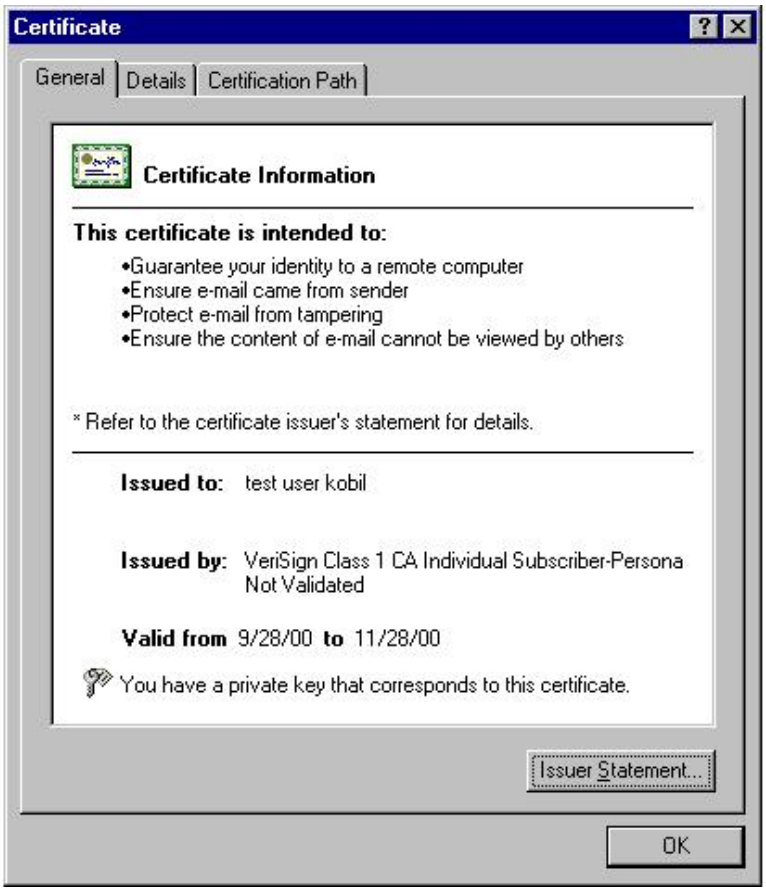
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended to:
•Guarantee your identity to a remote computer
•Ensure e-mail came from sender
•Protect e-mail from tampering
•Ensure the content of e-mail cannot be viewed by others
* Refer to the certificate issuer's statement for details.
Issued to: test user kobil
Issued by: VeriSign Class 1 CA Individual Subscriber-Persona Not Validated
Valid from 9/28/00 to 11/28/00
You have a private key that corresponds to this certificate.
Issuer Statement...
OK

Figure 2.4: Certificate details

2.1.3 Importing a CA Certificate

If you want to do secure communication with users of a new certification authority, you have to import its CA certificate (also called *root certificate*) first. If the CA certificate of a known certification authority expires, you also have to import the new CA certificate.

1. Download the CA certificate from the CA Web site.
2. Verify certificate integrity by checking that the fingerprint (a digest of the certificate) matches the fingerprint sent to you independently.
3. Add the CA certificate by the use of New Site Certificate dialog that prompts you.

Note that you automatically get an implicit trust relationship to all users of the new certification authority when you import its CA certificate! You should inform yourself about the certification poliy of the new certification authority before importing its CA certificate.

2.1.4 Importing another User's Certificate

Before you can send e-mail to a user, you must get the user's digital certificate and add it to your address book. You can obtain the certificate by two ways:

- Receive a signed e-mail from the user. Signed e-mail contain the user's digital certificate.
- Obtain the user's certificate from a public directory service:

Outlook Express

In Outlook Express, choose the menu

Edit > Find > People

Outlook 98 / 2000 / xp

In Outlook, click on **Find People** in the menu

Extras > Adress Book

Figure 2.5 shows the dialogue for all Outlook versions. You can search for the recipient's name or e-mail address.

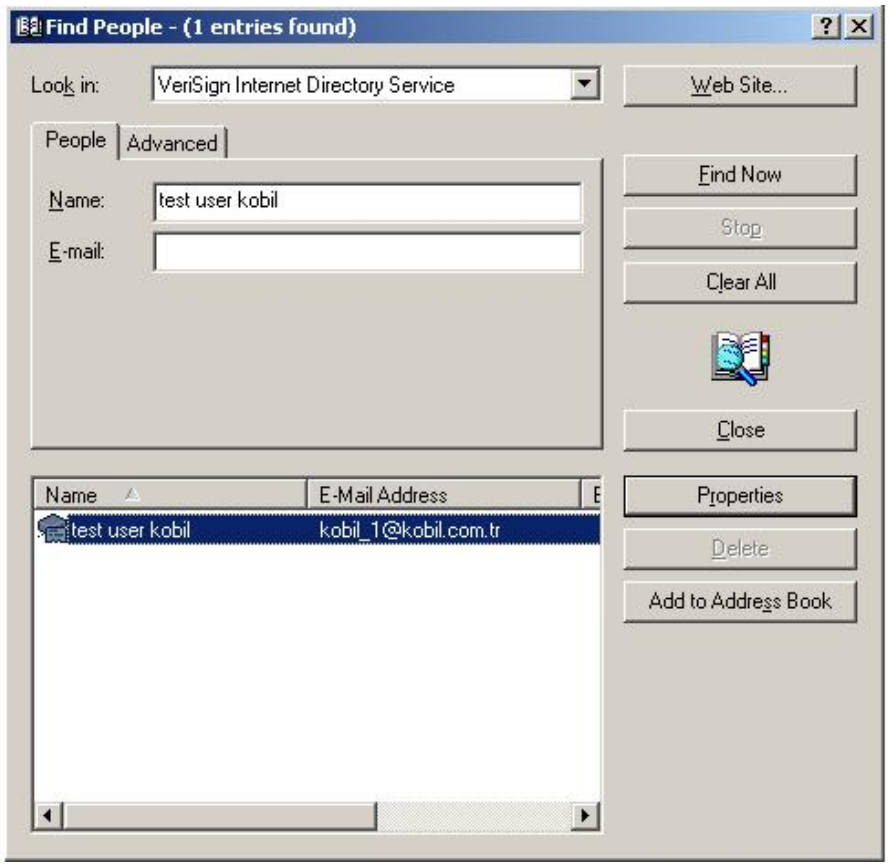

Figure 2.5: Find People Dialog

Setting-up a new directory service

If you want to use any other than the pre-installed directory services, open the menu

Extras > Accounts > Directory Service

and click on the button **Add > Directory Service...**. An assistant will be started that will guide you throught the process. You will have to enter the following informations:

- **Directory Server:** This is the address of the new directory server.
- **Authorization Required:** If this checkbox is active, you will have to enter a username and a password for user authentication. Usually, this option is not used.
- **Check Addresses with this Directory Service:** If this checkbox is active, the directory service will be used to resolve e-mail addresses from user names and to search automatically for recipient's certificates.

Once the directory service is configured, it may be necessary to enter the directory service's **Search Base**. To do that, select the newly installed directory service once more and click on **Properties**. In the drawer **Extended** you can enter the **Search Base**.

Ask your system administrator for the parameters suitable for your directory service.

You can also configure a directory service for **automatic Search for certificates** of e-mail recipients by activating in the menu

Extras > Accounts > Directory Service > Properties

tge option **Check recipient addresses with this directory service**.

Once you have successfully imported another user's certificate, you can take a look at it in the Windows certificate manager under **Other People** (see section 2.1.2).

2.2 Securing Internet Web Access using Internet Explorer

1. When your browser enters a secure site, you will get a security alert, if you did not disable this alert before.

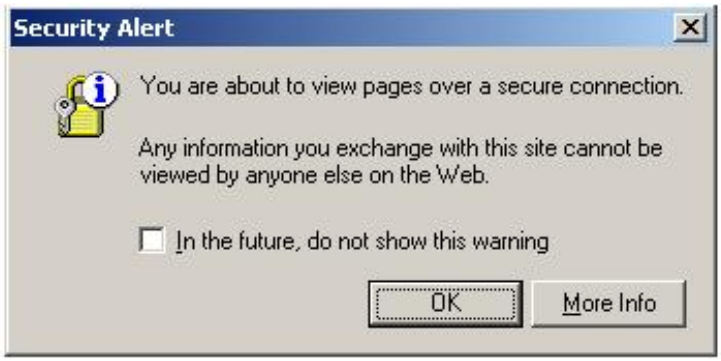
Security Alert
You are about to view pages over a secure connection.
Any information you exchange with this site cannot be viewed by anyone else on the Web.
In the future, do not show this warning
OK
More Info

Figure 2.6: Security Alert

2. The Web site responds with its certificate. Your browser checks the signature and other properties of this certificate. If the certificate has a security problem, you will get the following security alert:

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate is from a trusted certifying authority.
The security certificate date is valid.
The name on the security certificate does not match the name of the site.
Do you want to proceed?
Yes
No
View Certificate

Figure 2.7: Security Alert

3. If the web site wants you to authenticate yourself, you will be prompted with a client authentication dialog that lists all your certificates. If there is no certificate on the list, it means you do not have a certificate for this process. You can select and view any certificate before selecting the proper one. You can also press the **More Info** button to see Internet Explorer Help.

Figure 2.8: Client Authentication

4. If you select a certificate which belongs to KOBIL Smart Token, you will be prompted with a PIN entry dialog.

Figure 2.9: PIN entry dialogue

5. After a successful PIN entry, SSL connection will be accomplished. You should see the yellow lock on the status bar of Internet Explorer.

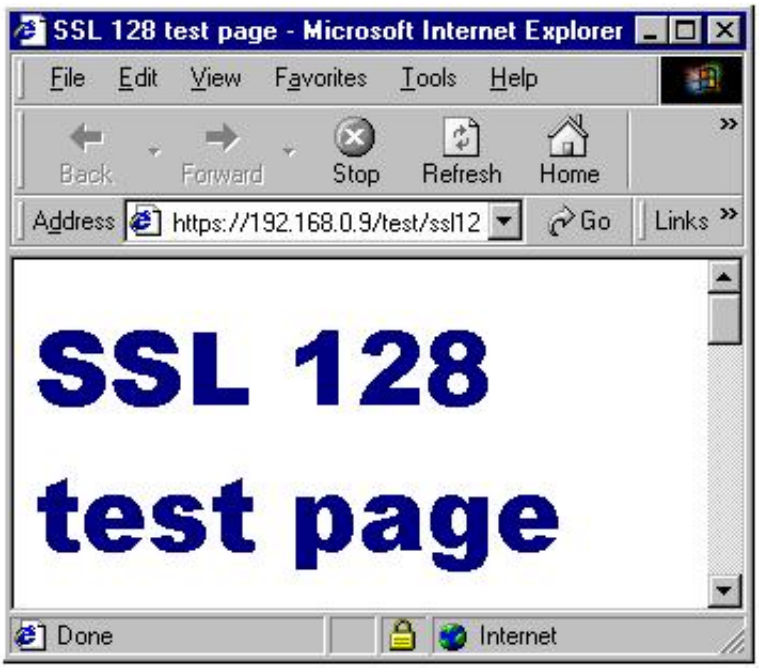

Figure 2.10: Secure Web Page

2.3 Secure E-mail Communication using Microsoft Outlook

In this section, you'll learn how to secure your e-mails using Microsoft Outlook Express, 98, 2000 and xp with KOBIL Smart Token.

We assume that both your internet access and e-mail account are properly configured. If you are not sure about this, contact your internet provider.

2.3.1 Choose your Certificate

To send signed messages and receive encrypted messages, you have to configure your e-mail certificate. If you don't select a default certificate and try to send a signed message, Outlook Express prompts you with a list of certificates to choose from.

The necessary steps differ a bit between Outlook Express and Outlook.

Outlook Express

In Outlook Express, your certificates are bound to your e-mail account, so you can select a default certificate for a each account.

1. Start Outlook Express and select

   Tools > Accounts

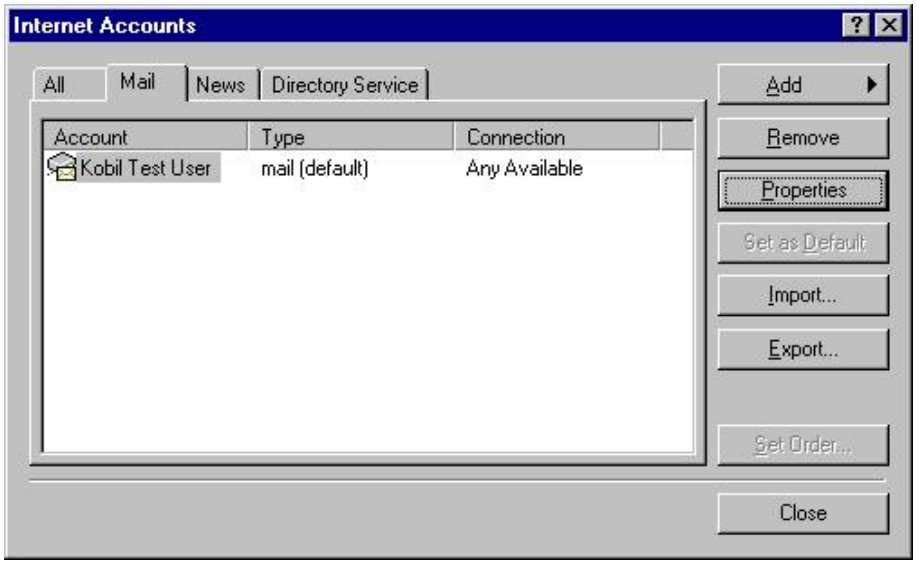

Figure 2.11: Internet Accounts Dialog

2. Choose your e-mail account as shown in figure 2.11 and click

   Properties > Security

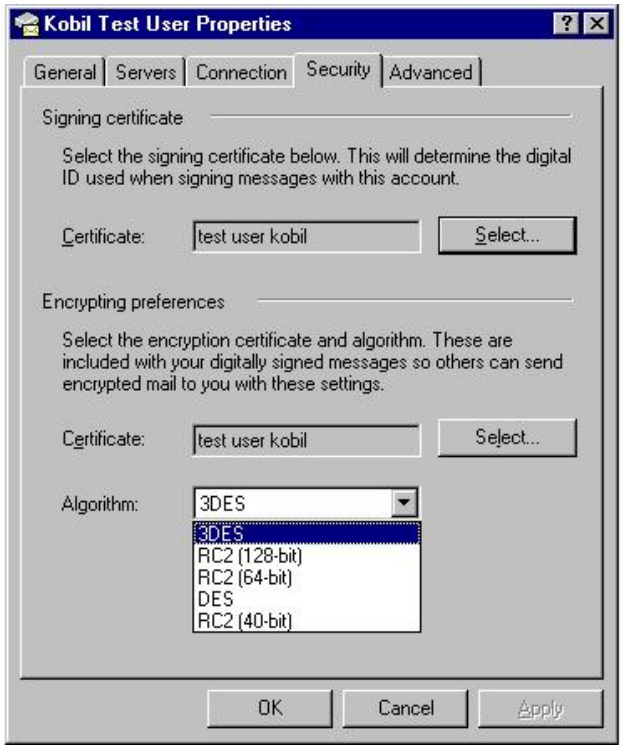

Figure 2.12: Internet Accounts properties Dialog

3. Click **Select** and choose a certificate from the list that shows all the certificates which can be associated with the account you selected above. If there are other certificates which don't have the same e-mail account information, they will not be displayed in this list. You can select the same certificate for signature and encryption if your security policy allows this. The dialogue is shown in figure 2.13.

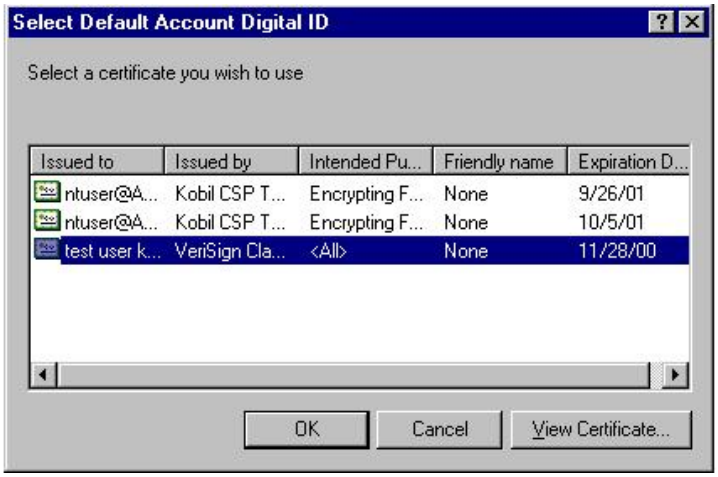

Figure 2.13: Select Digital ID Dialog

4. You can select the session key algorithm which will be used for bulk encryption and decryption. For strongest security, **3DES** or **RC2 128-bit** is recommended.

Outlook 98 / 2000 / xp

1. Start Outlook and choose the menu

   Extras > Options

2. Choose the drawer **Security** as shown in figure 2.14.

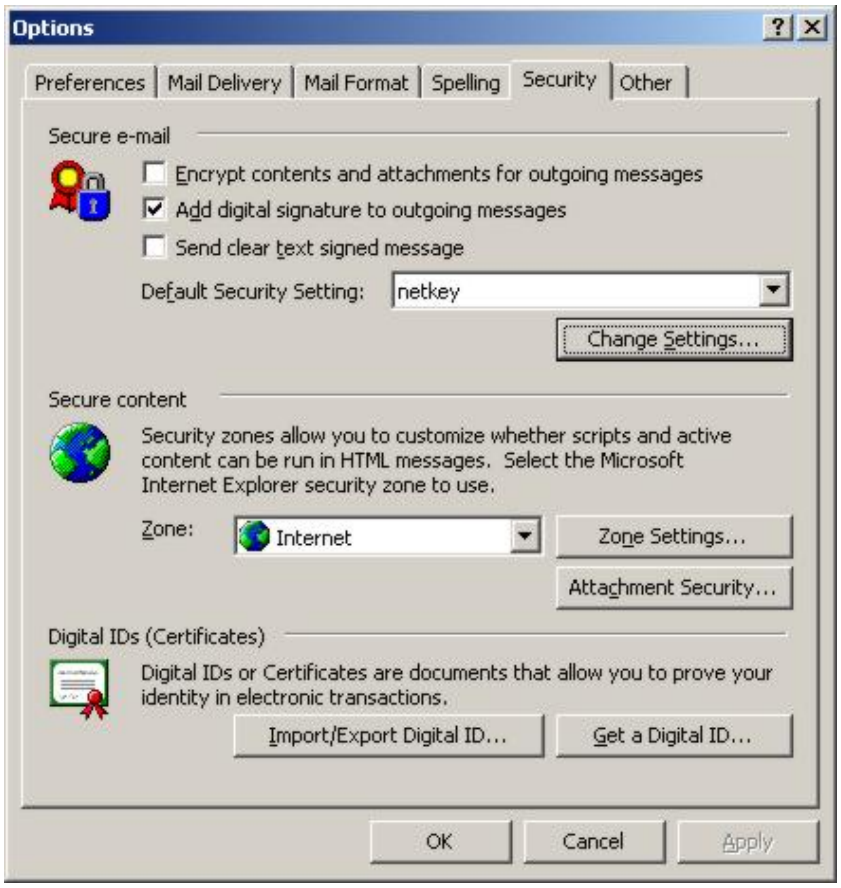

Figure 2.14: Security Options dialogue in Outlook

3. Click on the button **Change Settings...**. The dialogue shown in figure 2.15 will appear.

4. You can now select two independent certificates for signature and encryption using the **Choose...** buttons. **Be careful to select a certificate which contains the e-mail address suitable for your e-mail account!** You can select the same certificate for signature and encryption if your security policy allows this. The dialogue is shown in figure 2.13.

5. You can select the session key algorithm which will be used for bulk encryption and decryption as well as the hashing algorithm for digital signatures. For strongest security, **3DES** or **RC2 128-bit** is recommended as encryption algorithm and **SHA1** as hashing algorithm.

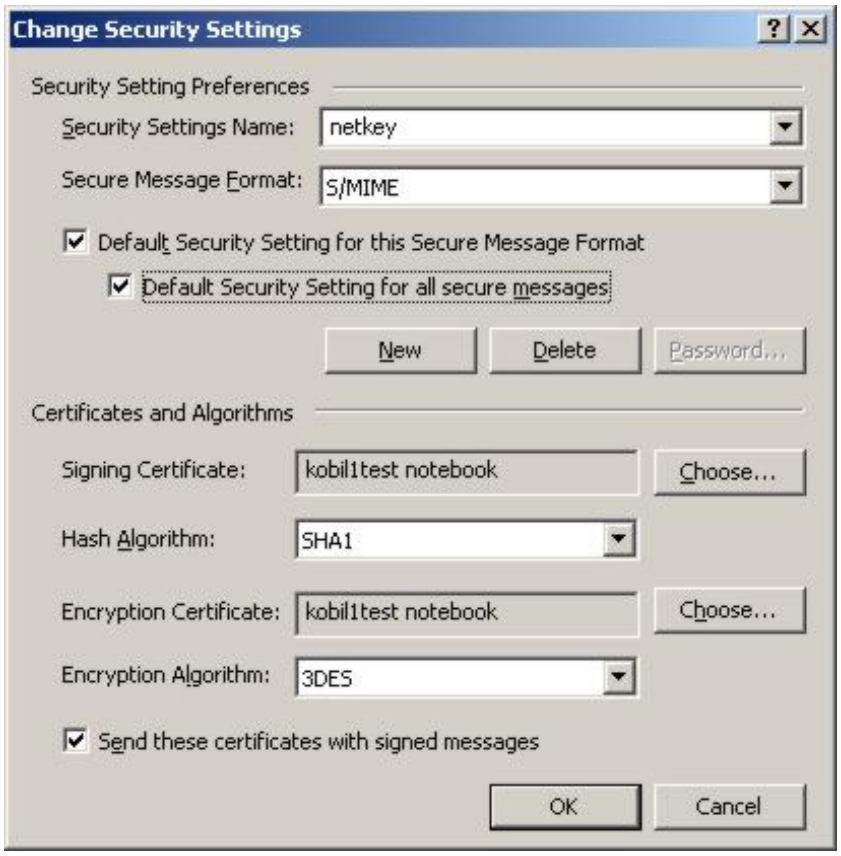

Figure 2.15: Outlook certificate selection

2.3.2 Sending secure E-mail

You can configure your default settings to sign and encrypt all outgoing messages (Click **Tools** > **Options** > **Security** and place checkmarks). If you do not define a default behaviour for signing and encryption, you can use **Sign** and **Encrypt** buttons of the new mail window. In Outlook, these buttons do exist, but are hidden by default. You can make them appear by configuring your menu bar.

To send a signed e-mail, you need a certificate associated with your account. You can choose a signing certificate as default. You should present your card and the PIN to sign the message. Your e-mail will be signed as soon as you click on the **Send** button.

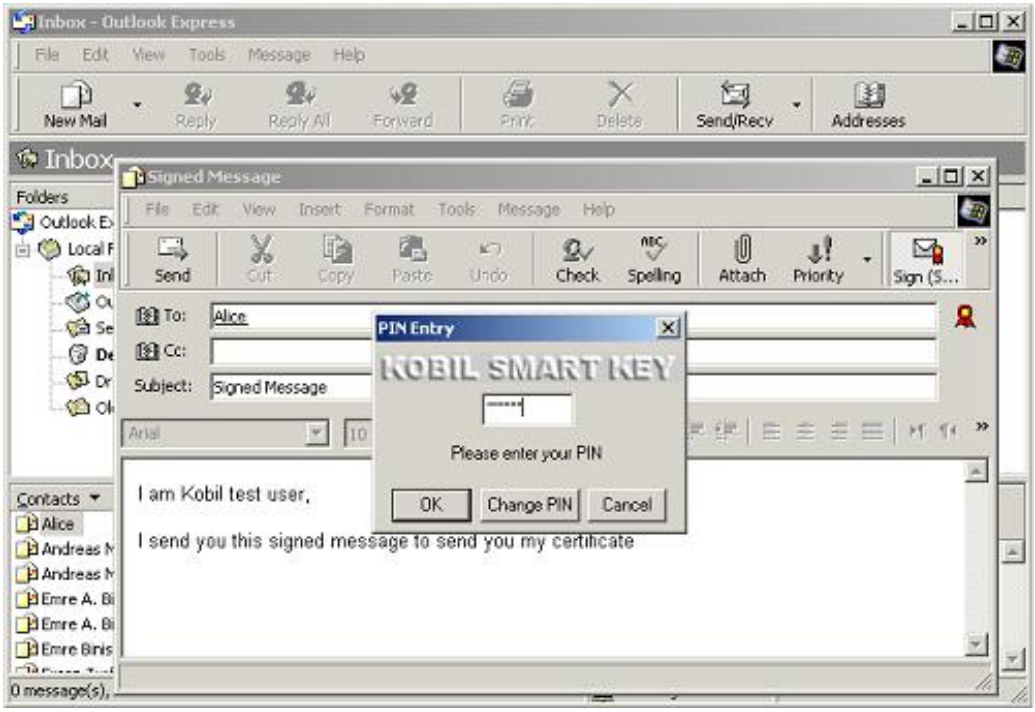

Figure 2.16: Signing an e-mail in Outlook Express

To send someone an encrypted message, you must have his/her certificate. You can also sign the encrypted message.

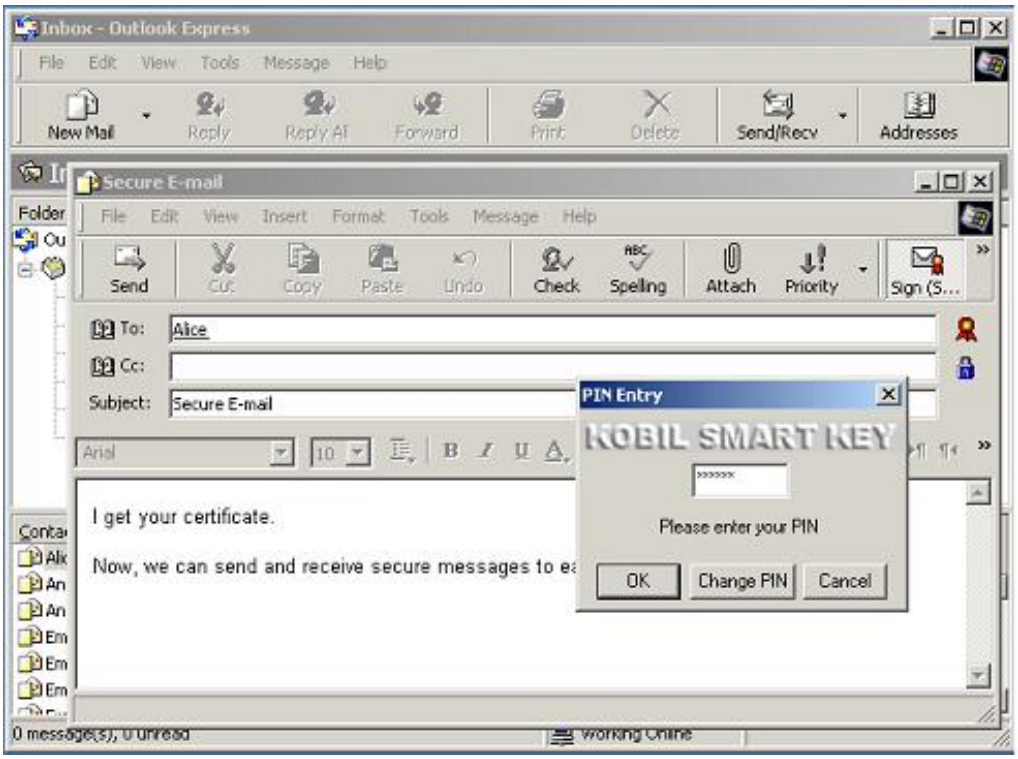
Inbox - Outlook Express
File Edit View Tools Message Help
New Mail Reply Reply All Forward Print Delete Send/Recv Addresses
Secure E-mail
File Edit View Insert Format Tools Message Help
Send Cut Copy Paste Undo Check Spelling Attach Priority Sign (S...
To: Alice
Cc:
Subject: Secure E-mail
Arial 10
I get your certificate.
Now, we can send and receive secure messages to ea
PIN Entry
KOBIL SMART KEY
Please enter your PIN
OK Change PIN Cancel
0 message(s), 0 unread
Working Online

Figure 2.17: Encrypting an e-mail in Outlook Express

2.3.3 Receiving secure E-mail

When you received a signed message, your browser makes the necessary checks to verify if the sender's certificate and the signature of the message are valid. If someone has your certificate, she can send you encrypted messages. You should present your card and the PIN to decrypt the message.

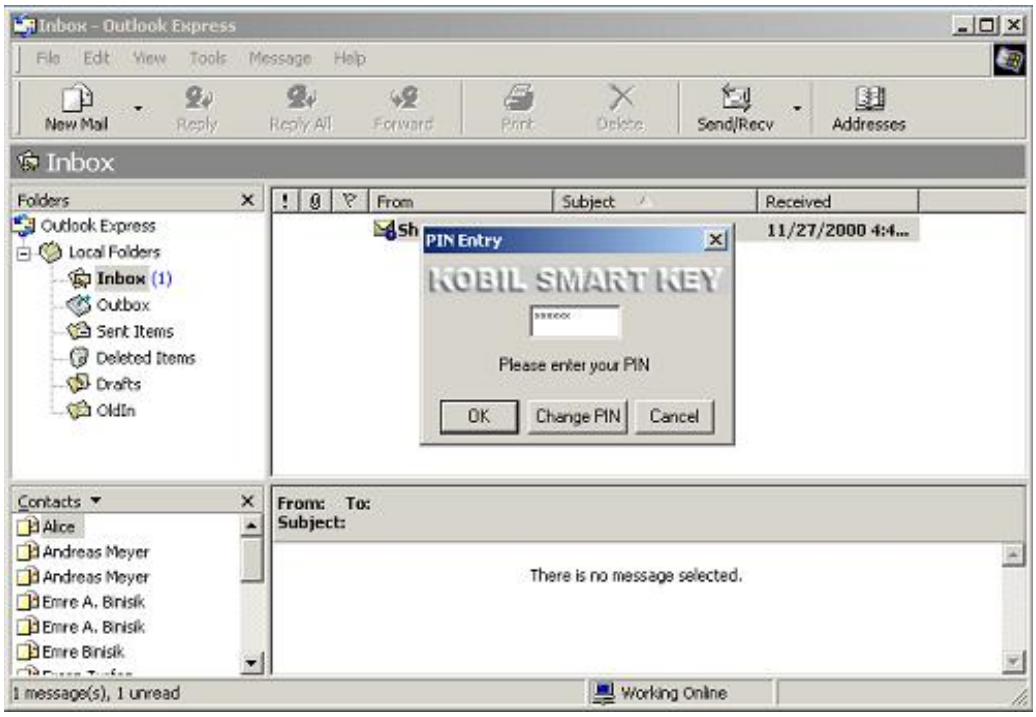

Figure 2.18: Receiving an encrypted E-mail in Outlook Express

Outlook Express shows encrypted messages with a blue sign and signed messages with a red sign. After a message signature is verified and the message is decrypted, you should click the **Continue** button (at the bottom of the e-mail) to see the mail content.

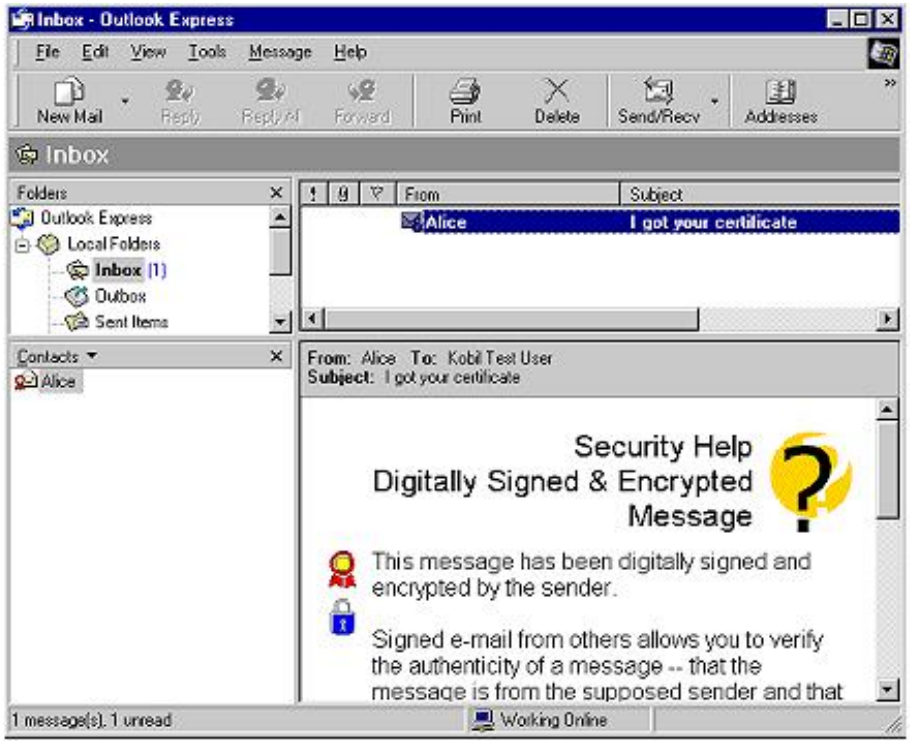
Inbox - Outlook Express
File Edit View Tools Message Help
New Mail Reply Reply All Forward Print Delete Send/Recv Addresses
Inbox
Folders
Outlook Express
Local Folders
Inbox (1)
Outbox
Sent Items
From Subject
Alice I got your certificate
Contacts
Alice
From: Alice To: Kobil Test User
Subject: I got your certificate
Security Help
Digitally Signed & Encrypted Message
This message has been digitally signed and encrypted by the sender.
Signed e-mail from others allows you to verify the authenticity of a message -- that the message is from the supposed sender and that
1 message(s), 1 unread
Working Online

Figure 2.19: Receiving a signed e-mail in Outlook Express

2.4 The Token Manager

Token Manager is a utility that contains the following functions required to manage your SIM cards and the certificates on them:

1. **Delete certificates from your SIM card**
   If you don't need a certificate anymore, you can delete it from your SIM card using Token Manager
2. **Import certificates onto your SIM card**
   Existing software certificates and corresponding private keys can be loaded onto your SIM card. This can be necessary during a migration from software- based certificates to smartcards, but note that this is somewhat risky, since the private keys have not been stored inside the security environment of your SIM card without interruption!
3. **Change the SIM card's PIN**
4. **Unblock the SIM card's PIN** using the SIM card's PUK.

You can start Token Manager using

Start Menu > Programs > KOBIL Systems > KOBIL Smart Token > Token Manager

Figure 2.20 shows the Token Manager dialogue.

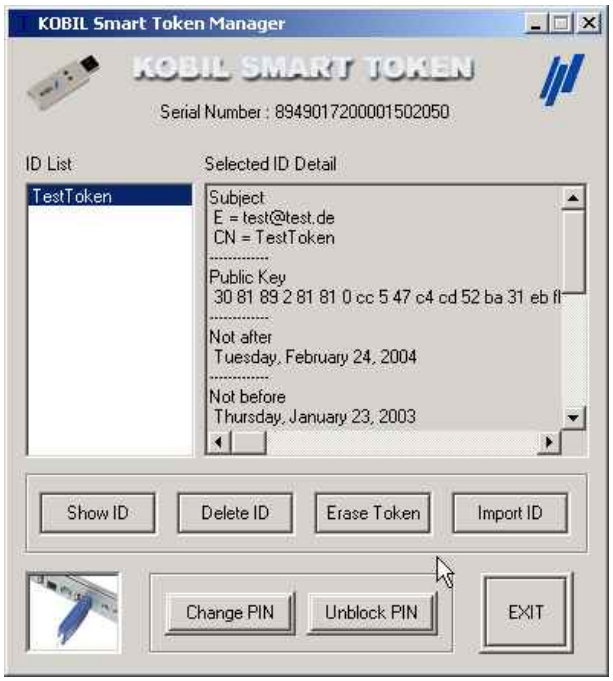

Figure 2.20: Token Manager

2.4.1 Delete certificates from your SIM card

Be very careful with certificate deletion, since any data encrypted with that certificate cannot be recovered after!

Choose the certificate to delete click on **Delete ID**. If you want to erase the whole token, please click on **Erase Token**.

2.4.2 Import certificates onto your SIM card

KOBIL Smart Token allows you to load software-based certificates (e.g. certificates and private keys stored in PKCS#12 files) from the windows certificate manager onto your TCOS smart card if they are marked as **exportable**. To do so, click on the **Import Cert** button in the **Card** drawer.

If you have your software-certificate only as a PKCS#12 file (e.g. a file whose name ends with **.p12**), you'll have to import it into the windows certificate manager first by double-clicking it. Follow the instructions of the windows certificate manager during the import and mark the private key as **exportable**.

For security reasons, the software certificate is deleted from the windows certificate manager after successfully importing it onto your SIM card!

Depending on your configuration, this function may be disabled.

2.4.3 Changing and Unblocking the SIM card's PIN

If you want to change your SIM card's PIN, click on the **Change PIN** button. You will have to enter your old PIN and then the new PIN twice.

Depending upon your configuration, you have the possibility to unblock the PIN using a PUK as you may know from your mobile phone SIM card. This may become necessary if your PIN is blocked after three wrong entries. You can do this by clicking the **Unblock PIN** button.

Chapter 3

Smart card Logon for Windows 2000/XP

In this section, you'll learn how Windows 2000 and Windows XP/.net Server networks are secured by smartcard logon using KOBIL Smart Token. The users will be able to log in with their SIM cards into the network instead of static passwords.

To be able configure Windows for smartcard login, one must have deeper knowledge about Windows administration. In this manual, we can only show the steps concerning directly KOBIL Smart Token. Further configuration, e.g. policy settings, may be necessary to satisfy your particular security policy.

3.1 Prerequisites

Windows 2000 and XP make it possible to deploy strong authentication using smart cards by leveraging operating system features such as Kerberos, Active Directory, and the variety of administrative tools used to manage a public key infrastructure. To use the smart card logon feature, you can pursue the following steps or you can get more information from Windows 2000 / .net Server help.

1. **A PCSC driver for your KOBIL smartcard terminal must be installed on every client machine! A CT-API driver will not work.** To find out if a PCSC driver is installed, open the device manager in the system configuration panel and take a look if a KOBIL smartcard terminal appears there. If not, you'll have to install a PCSC driver first.
2. Install at least one Windows 2000 / .net Server in your network as a domain controller.
3. Install the following optional components on your server in the same order:
   (a) Domain Name Service (DNS)
   (b) Active Directory
   (c) Certification Authority
4. Logon into domain as Administrator.
5. If you want to issue smart cards from another computer, make sure that DNS is configured correctly and that this computer is member of the domain.
6. Get and install an Enrollment Agent Certificate (see section 3.2).
7. Define users in Active Directory.
8. Issue a smart card logon certificate for each user (see section 3.3).

3.2 Enrollment Agent Certificate

An administrator needs an Enrollment Agent Certificate to issue Smart Card Logon Certificates. Follow these steps to get an enrollment agent certificate. If you logon from a different computer than the server, make sure that this computer is correctly configured as a domain member.

1. Run the Certificate Authority from the start menu:
   Start > **Programs** > **Administrative Tools** > **Certificate Authority**
2. Right-click **Policy Settings** under the name of your CA and select
   New > **Certificate to issue**

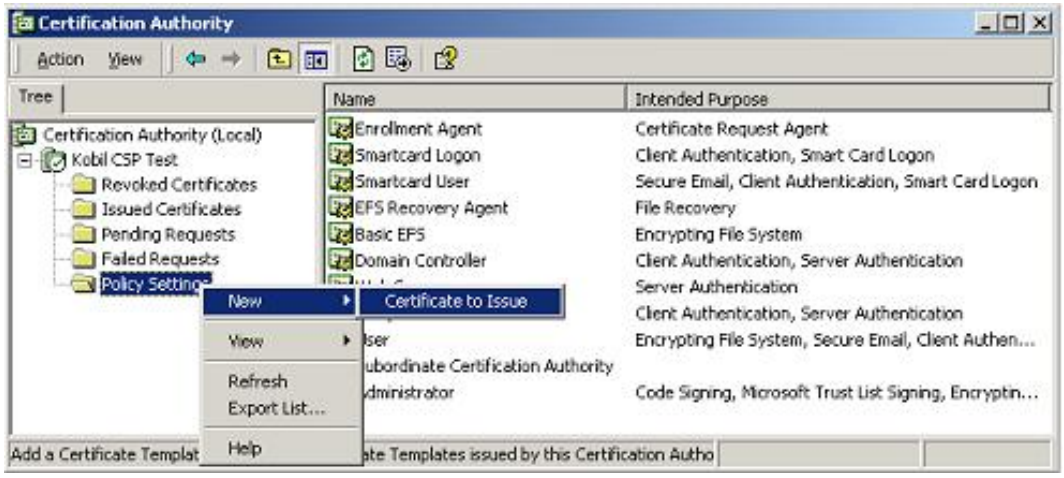

Figure 3.1: Certificate Authority

3. Add those Certificate Templates from the list: **Enrollment Agent**, **Smartcard Logon** and **Smartcard User**.

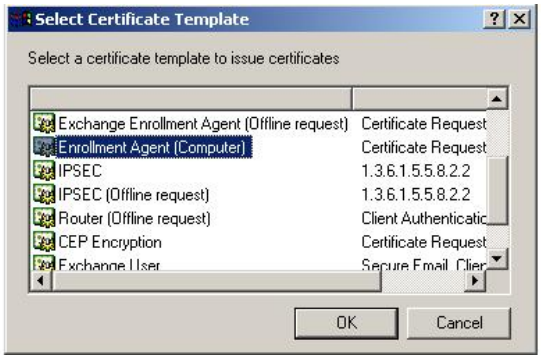

Figure 3.2: Certificate Templates

4. Close the Certification Authority console.
5. Run Microsoft Management Console (*mmc* from the command prompt).

6. Click **Console** > **Add/Remove Snap-in**

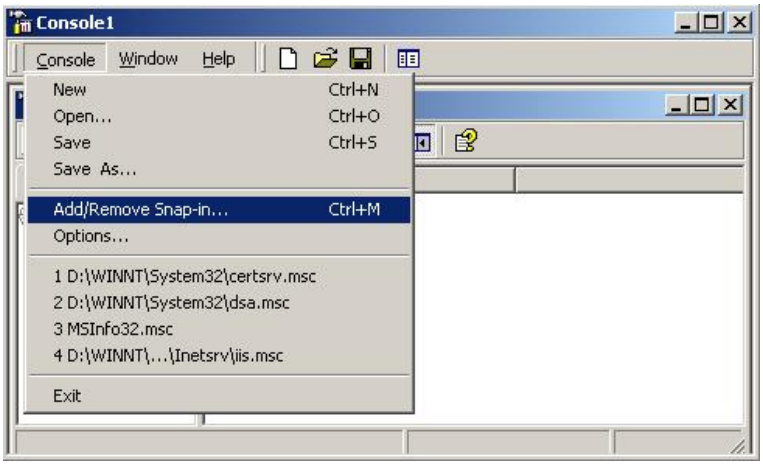

Figure 3.3: Add/Remove Snap-in in the MMC

7. Click **Add**, select **Certificates**, click **Add**, select **My User Accounts**, click **Finish** > **Close** > **Ok**

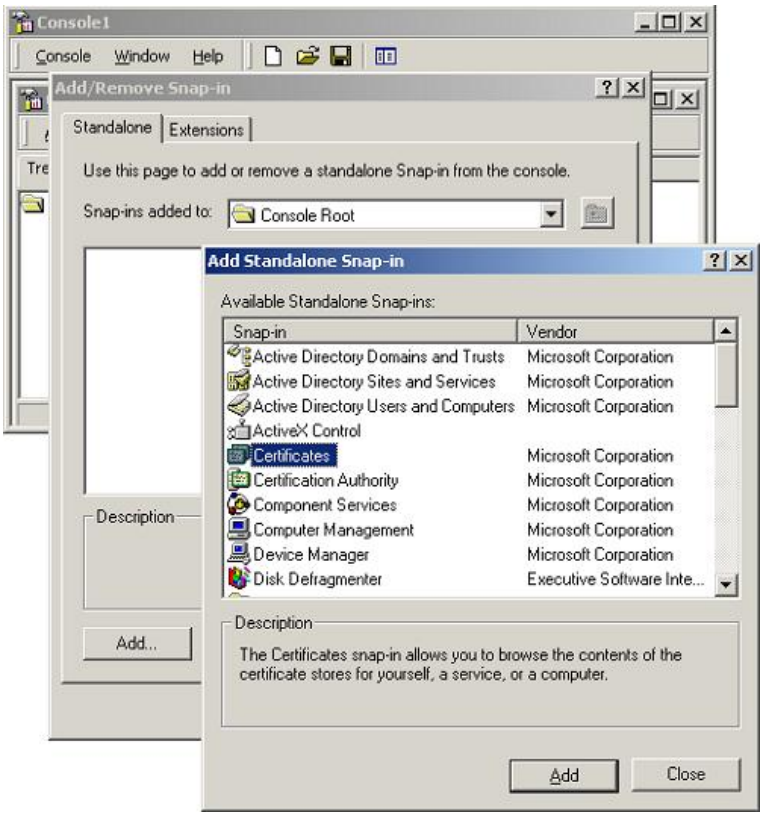

Figure 3.4: Adding Snap-in

8. Right click on **Personal** under **Certificates** and select **All Tasks** > **Request New Certificate...** from the menu. The Certificate Request Wizard will be started.

Figure 3.5: Request New Certificate

9. Click **Next**, select **Enrollment Agent** from certificate templates, click **Next**, write a **friendly name**, click **Next** > **Finish** > **Install**

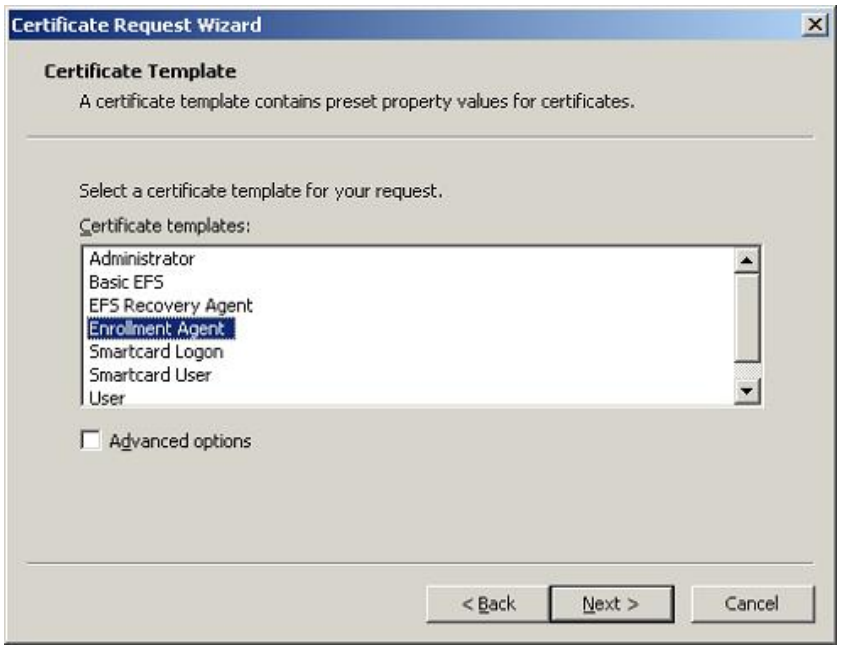

Figure 3.6: Certificate Request Wizard

3.3 Issuing Smart Card Logon Certificates

These steps have to be performed for each user who shall obtain a smart card for login.

1. The Administrator who has the Enrollment Agent Certificate must logon into the CA web page by using Internet Explorer. The address is

   http://x.x.x.x/certsrv (x.x.x.x is the server's DNS address)

Figure 3.7: Password Dialog

2. Select **Request a certificate** and click **Next**

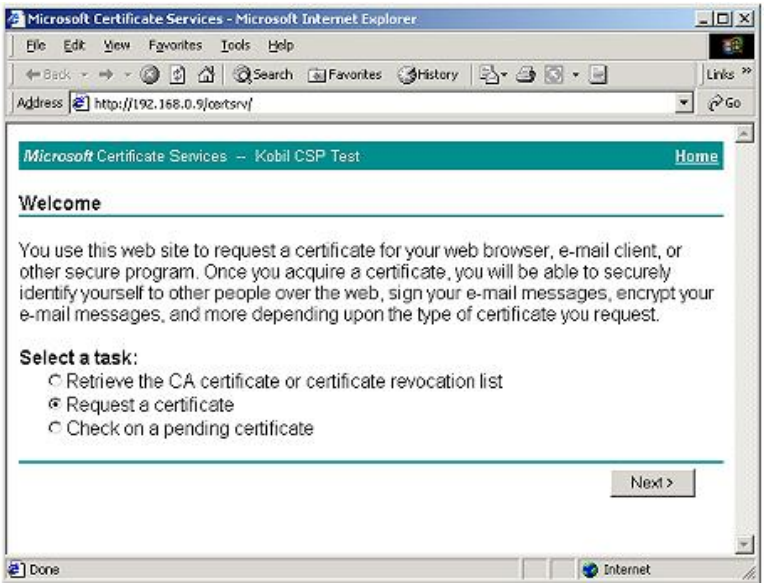
Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Search Favorites History
Address http://192.168.0.9/certsrv/
Microsoft Certificate Services -- Kobil CSP Test
Home
Welcome
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.
Select a task:
Retrieve the CA certificate or certificate revocation list
Request a certificate
Check on a pending certificate
Next >
Done
Internet

Figure 3.8: Microsoft Certificate Service

3. Select **Advanced Request** and click **Next**

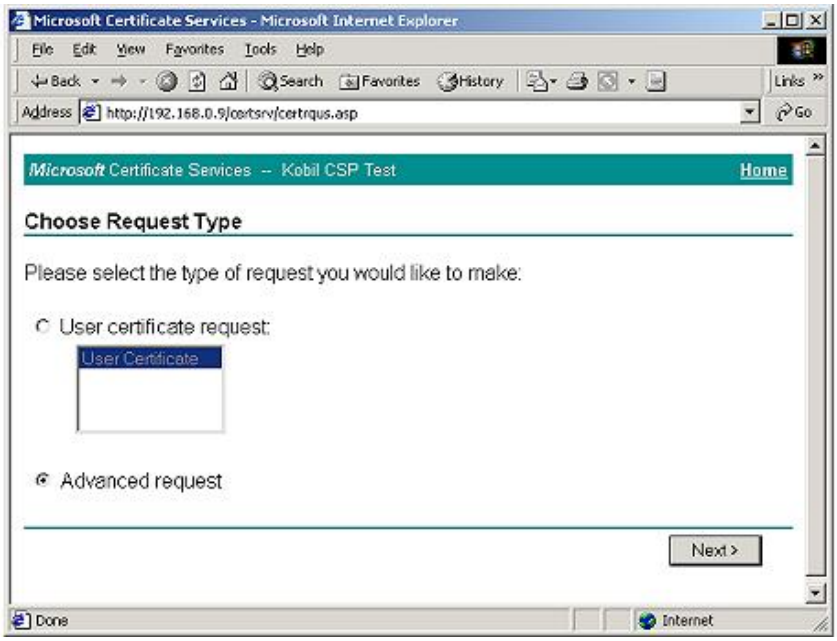

Figure 3.9: Choosing Request Type

4. Select **Request a certificate for a smart card** and click **Next**

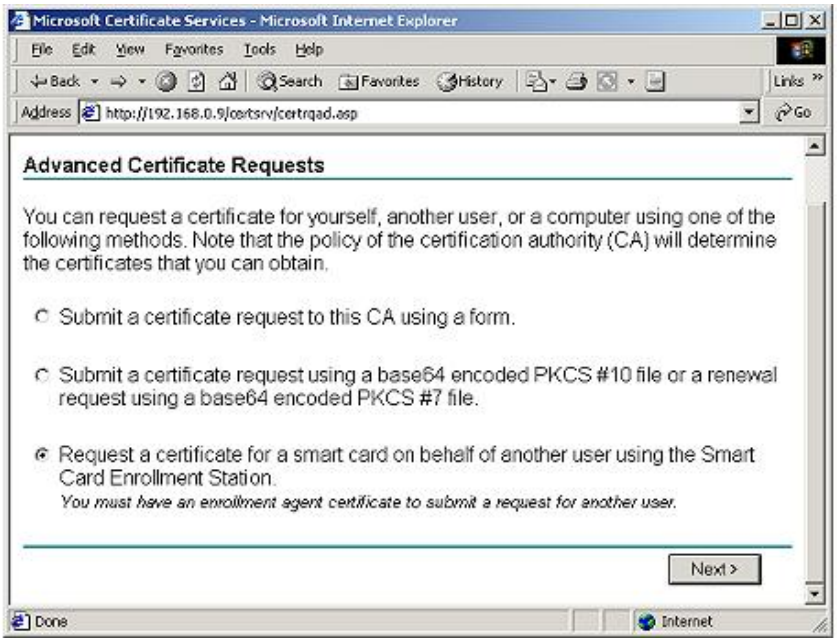

Figure 3.10: Advanced Certificate Request

5. Select the template **Smart Card Logon**, your CA as Certification Authority and **KOBIL Smart CSP v1.0** as CSP. Your enrollment agent certificate should be selected under **Administrator's Enrollment Agent Certificate**. Select the **user** to be enrolled from Active Directory. Insert an empty SIM card and click **Enroll**. You will be prompted for the card's PIN. After enrollment is finished, you can view the logon certificate and continue the same process for another user with another card.

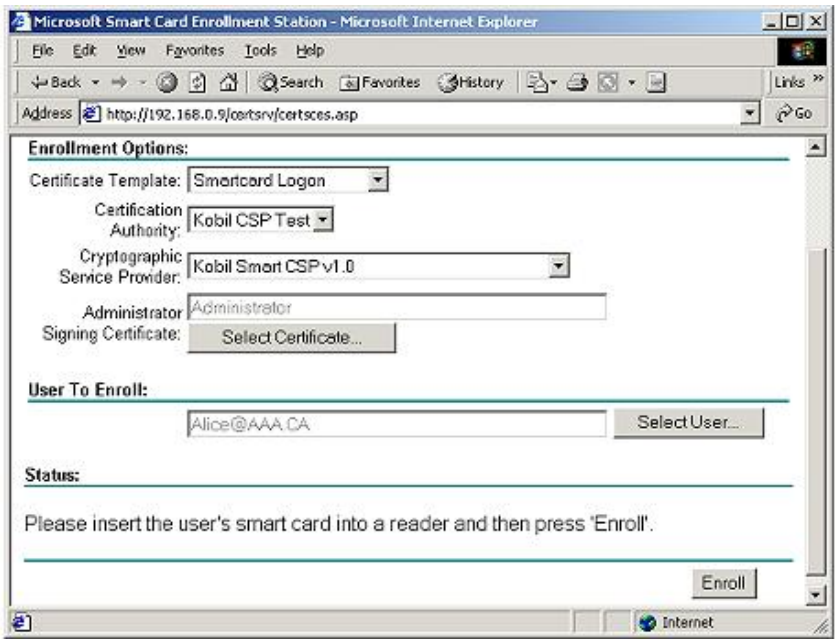

Figure 3.11: Enrollment Options

3.4 The Smart Card Logon Process

If Windows 2000 or XP detects a PC/SC compatible reader at start up, it gives the option to use a smart card for logon instead of a password.

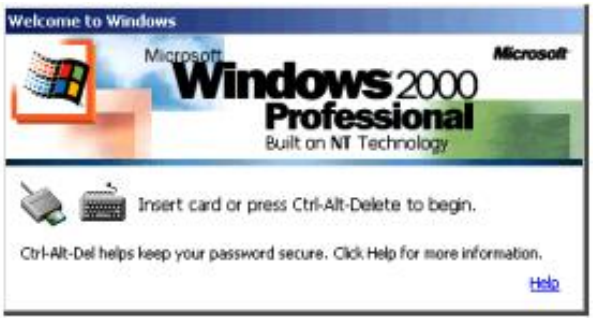

Figure 3.12: Windows 2000 Logon Dialog

Interactive Logon using a smart card begins with the user inserting a smart card into a smart card reader. After this, Windows will prompt for a Personal Identification Number (PIN) instead of a username, domain name and password. The card insertion event is equivalent to the familiar *Ctrl +Alt + Del* sequence used to initiate a password-based logon. However, the PIN the user provides to the logon dialog is used to authenticate only to the smart card and not to the domain itself. The logon certificate in the smart card is used to authenticate the user to the domain.

Figure 3.13: PIN Entry Dialog

If smartcard login fails with some error dialogues, please take a look at section A.1.

3.5 Smartcard-Login in Citrix Metaframe XP Environments

Using KOBIL Smart Token, you can also secure Citrix Metaframe XP FR2 terminal clients. Starting with FR2, Citrix Metaframe XP is able to forward PC/SC connections from the terminal client to the terminal server, so it is only necessary to install KOBIL Smart Token on the server and PC/SC drivers on the clients.

Further information can be found in the KOBIL Integration Guide *Integrating KOBIL Smart Token with Citrix Metaframe* which you can obtain from KOBIL.

Chapter 4

Using the KOBIL Smart Token PKCS#11 Module for Netscape

The KOBIL Smart Token PKCS#11 module was optimized for usage with Netscape Communicator, but you can use it also independently from Netscape.

4.1 Certificate Management with Netscape

Netscape has a build-in certificate manager that runs independenty from the windows certificate manager on windows platforms. In this section, you learn about the Netscape certificate manager.

4.1.1 Getting your Certificate

You must follow these steps if you do not have a certificate on your SIM card yet. However, in some cases **you get a personalized SIM card from you card issuer** that already holds your certificate. In these cases, you don't need to request a certificate and you can skip this section.

1. Insert your KAAN SIM into your computer's USB port. The SIM card is already inserted into KAAN SIM (see section 1.3).
2. Start Netscape Communicator
3. Surf to a certification authority of your trust, for example:
   - TeleSec Trustcenter (Germany): www.telesec.de
   - TC Trustcenter (Germany): www.trustcenter.de
   - Verisign (USA): www.verisign.com
4. Most of these certification authorities offer free trial certificates (often also called *Digital ID's*). You may choose a trial certificate, but note that this kind of certificates does not offer a high security level.
5. Enter some data that are required for your certificate (depending on the certification authority), for example:
   - Some personal data including your email address.
     It is really important that you enter your email address correctly (also case-sensitive!) as configured in you email account. Otherwise, you wont't be able to use your certificate!

- Choose **RSA, 1024 Bit** as key type and size.

6. Start the enrollment procedure by clicking the **Submit** button.

7. Now, Netscape will open a dialogue to ask in which **card or database** the new key will be stored as shown in figure 4.1. Choose **KOBIL Smart Token**.

Private Key erstellen - Netscape
Private Key erstellen
Klicken Sie auf "OK". Für Ihr Zertifikat wird nun ein Private Key erstellt
Dies kann einige Minuten dauern.
Wichtig: Wird dieser Vorgang unterbrochen, müssen Sie das
Zertifikat erneut anfordern.
Wählen Sie die Karte oder Datenbank, mit der der Schlüssel generiert
werden soll:
KOBIL Smart Token
KOBIL Smart Token
Communicator Certificate DB
Mehr Info...
OK
Abbrechen

Figure 4.1: Key Generation Window

8. **If your SIM card has not yet a PIN**, you will have to initialize it now. Otherwise, **if your SIM card already has a PIN**, you are now asked to enter it.

Figure 4.2: PIN-entry dialogue

9. Now, your key pair is being generated on your computer and written to your SIM card. This process is rather complex and may take some seconds.

10. Once the public key is successfully transmitted to the CA, you will either get your certificate immediately on the next web page or it will be sent to you by e-mail.

11. Follow your CA's instructions to import and install the certificate. If it does not install automatically, the installation procedure should be described by the CA. Finally your certificate will be written into your SIM card.

12. Now, you can take a look on your new certificate under

    Communicator > Extras > Security Options > Certificates > Yours

    as shown in figure 4.3. For details see section 4.1.2.

13. In some cases, you have to import the **root certificate of your teustcenter**, if it is not yet present in the Netscape certificate manager. For details, see section 4.1.3.

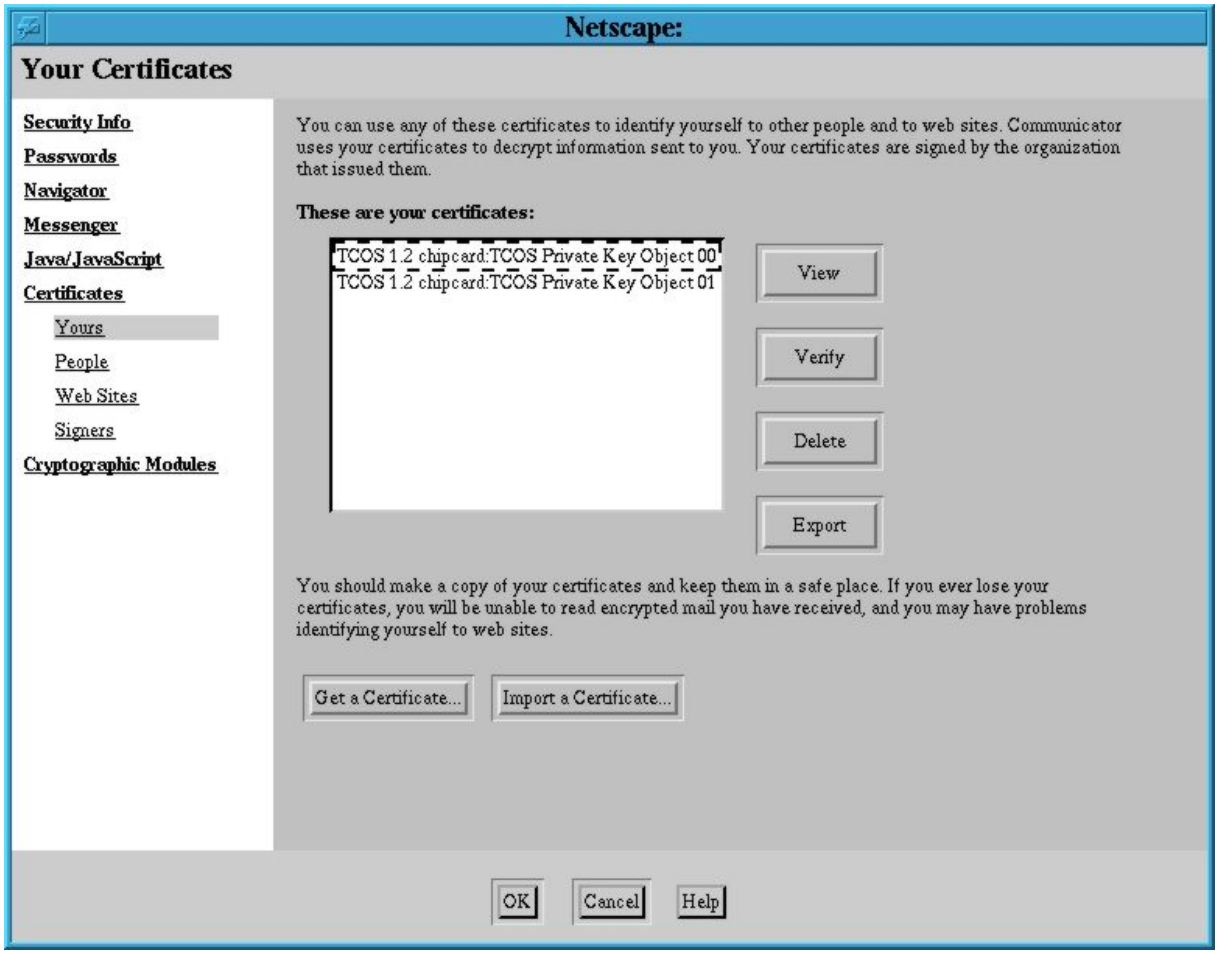
Netscape:
Your Certificates
Security Info
Passwords
Navigator
Messenger
Java/JavaScript
Certificates
Yours
People
Web Sites
Signers
Cryptographic Modules
You can use any of these certificates to identify yourself to other people and to web sites. Communicator uses your certificates to decrypt information sent to you. Your certificates are signed by the organization that issued them.
These are your certificates:
TCOS 1.2 chipcard:TCOS Private Key Object 00
TCOS 1.2 chipcard:TCOS Private Key Object 01
View
Verify
Delete
Export
You should make a copy of your certificates and keep them in a safe place. If you ever lose your certificates, you will be unable to read encrypted mail you have received, and you may have problems identifying yourself to web sites.
Get a Certificate...
Import a Certificate...
OK
Cancel
Help

Figure 4.3: User certificates

Specifically note, that the number of certificates you can store on your smart card mainly depends on the available memory. We implemented an upper limit of 10 certificates, however with a 16KB TCOS 2.0 smart card, you usually can put a maximum of 6-8 certificates onto one card (depending on the length of the individual certificates). To remove a certificate, use the procedure described in section 4.1.2.

4.1.2 Managing Certificates

In this section, you'll learn how to manage your certificates using the Netscape certificate manager. You can open Netscape's certificate manager in two ways:

- In Navigator (web browser) using the button **Security**
- In Messenger (email client) over the menu

Communicator > Extras > Security Options

The dialogue shown in figure 4.3 appears when you click on **Certificates**. Now, you have access to the Netscape certificate database where 4 individual types of certificates are stored:

1. Your own certificates (**Yours**)
2. Other people's certificates (**Others**)
3. Web server certificates (**Web-Sites**)
4. CA certificates (**Signers**)

Your own certificates (Yours)

Open the Netscape certificate manager (see section 4.1.2) and click

Certificates > Yours

Now, all your certificates are displayed as in figure 4.3. Your certficates are the ones where you possess the appropriate private key.

- The button **View** shows certificate details.
- The button **Verify** checks if the choosen certificate is valid.
- The button **Export** exports the choosen certificate with the corresponding private key. **Note that this function is not supported by KOBIL Smart Token, since you are not able to read out your private key from your SIM card for security reasons.**
- You can delete the choosen certificate with the button **Delete**. **Be careful with deletion of your certificates, because after that, you cannot decrypt any messages encrypted with that certificate!**

Other people's certificates (Others)

Open the Netscape certificate manager (see section 4.1.2) and click

Certificates > Others

Now, all known certificates from other people are displayed as in figure 4.4.

- The button **View** shows certificate details.
- The button **Verify** checks if the choosen certificate is valid.
- You can delete the choosen certificate with the button **Delete**. **Be careful with deletion of other people's certificates, because after that, you cannot encrypt messages to this person, before you import it again (see section 4.1.4).**
- With the button **Search Directory** you can search for other people's certificates in a public directory service as described in section 4.1.4.

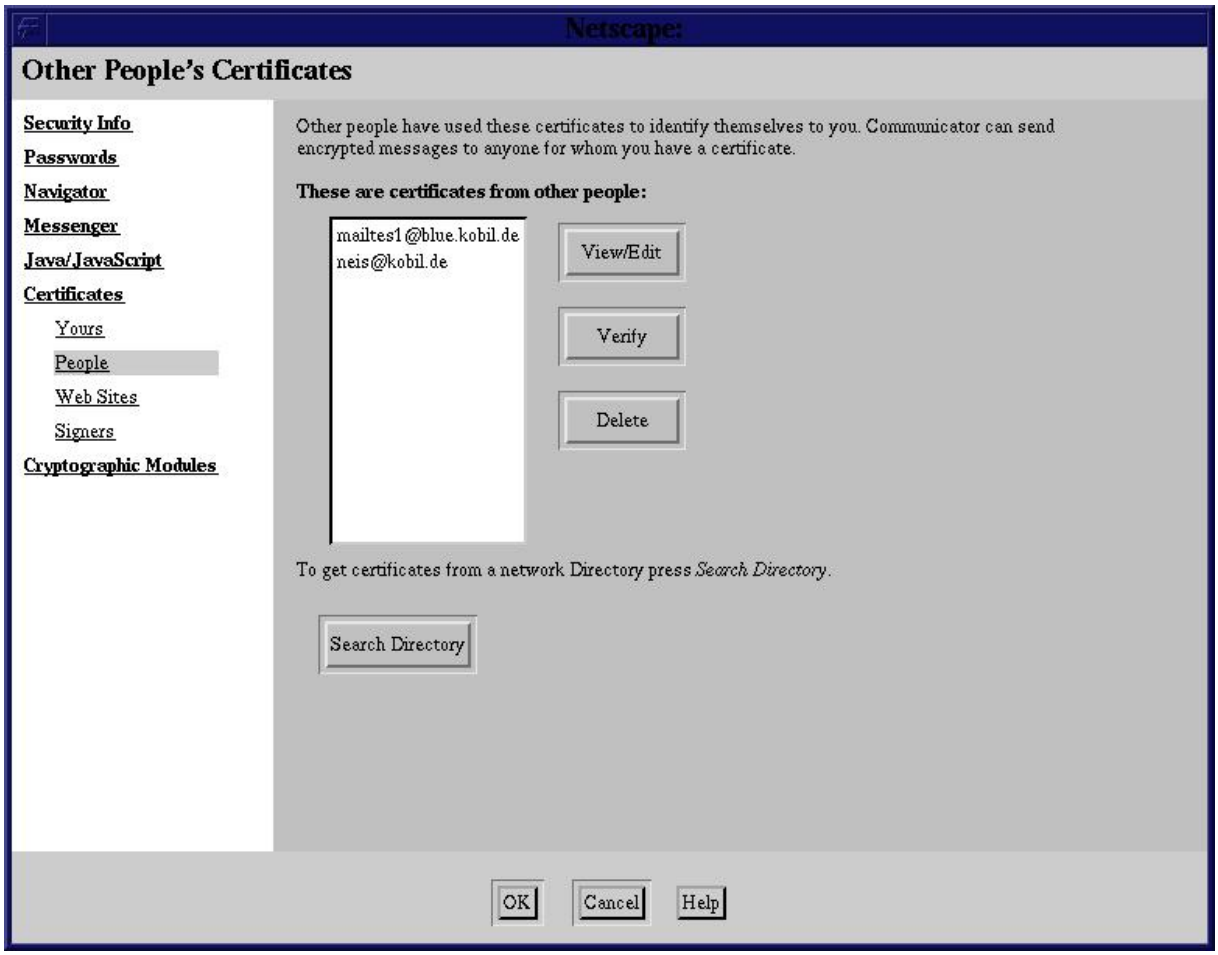

Figure 4.4: Other People's Certificates

Web server certificates (Web-Sites)

Open the Netscape certificate manager (see section 4.1.2) and click

Certificates > Web-Sites

Now, all known certificates from web servers are displayed. They can be managed just like other people's certificates.

CA certificates (Signers)

To make use of other peoples certificates, e.g. to verify their signatures, to send encrypted emails to them or to communicate via secured SSL connections, you need to know their certificate. However, if you try to obtain their certificates, anybody could intercept that connection and pass you whatever certificate he likes, so later somebody might intercept all the communication that you believe to be safe from such attacks.

To prevent this problem, certificates are required to be signed by some trustworthy instance, a so called certificate signer. That way you can verify the certificate's signature and know that nobody is giving you a wrong certificate - at least not without the active support of such a certificate signer.

Thus choosing the certificate signers that you accept is of critical importance. Netscape has a number of built-in certificate signers that you can see by clicking on

Security > Certificates > Signers

To know how to import a new CA certificate, see section 4.1.3.

4.1.3 Importing a new CA Certificate

Sometimes, you might feel the need to accept an additional certificate signer, for example if your bank is using a self-signed certificate for online banking.

In such cases, you can direct Netscape to the certificate signers site and install its certificate by clicking on a specific link. A sequence of dialogues will appear informing you that you are about to import a new CA certificate and that this is an important security operation. You will have to activate the purposes for which this CA will be enabled. Note that by default, no such purpose is active, so that you have to activate at least one purpose before you can use that CA certificate.

Note that you automatically get an implicit trust relationship to all users of the new certification authority when you import its CA certificate! You should inform yourself about the certification poliy of the new certification authority before importing its CA certificate.

4.1.4 Importing another User's Certificate

To send someone a secure mail, you need to add this person's certificate to your "Other People" certificates list (see figure 4.4). This can be done in two ways:

- You receive a signed e-mail from the other user. His certificate is included in each signed e-mail and will be imported automatically into the "Other People" certificate list.
- If you don't have received any signed e-mail from the other user yet, you can search for it in a public **Directory Service** which is kind of a phone book for certificates. You can search a directory service by clicking the button **Search Directory**. As search criteria, you can enter the other user's name or e-mail address. If you want to use any other than the pre-configured directory services, you will have to open your Netscape address book first via the menu

  Communicator > Adress Book

  and add the new directory service there by choosing the menu

  File > New Directory...

For the necessary parameter settings for your particular directory service, ask your system administrator.

You can also configure a directory service for **automatic search for certificates** of e-mail recipients by selecting the particular directory service in the menu

Edit > Preferences > Mail & News > Adressing

under **automatic address completion**.

4.1.5 Importing a Web Server's Certificate

If you surf on a secured web site (with the "*https://*"-prefix) whose server's certificate is not yet known under **Certificates > Web-Sites** and whose CA is not known under **Certificates > Signers**, a web server certificate import dialogue appears. In all other cases (web server's certificate is already known, web server's CA is already known), this dialogue will not appear.

During the dialogue you are advised that you are about to trust a new web server. You can either **accept this certificate forever (until it expires)** or **accept it only for this session**.

4.1.6 Changing the PIN of your SIM card

You can change your SIM card's PIN using the Token Manager, as described in section 2.4.

4.2 Secure Web Sessions using Netscape Navigator

Secure Sessions rely on the SSL protocol (see section B.3.7, so all secure web sites are accessed using the **https://** prefix.

If your browser does already have the server's certificate (and if your browser has a certificate to confirm your identity - e.g. if it is stored on the smart card) a secure session will be initiated, otherwise, your access request will be rejected.

While initiating the secure session, you will have to choose the certificate to be used in confirming your identity in the screen shown in figure 4.5.

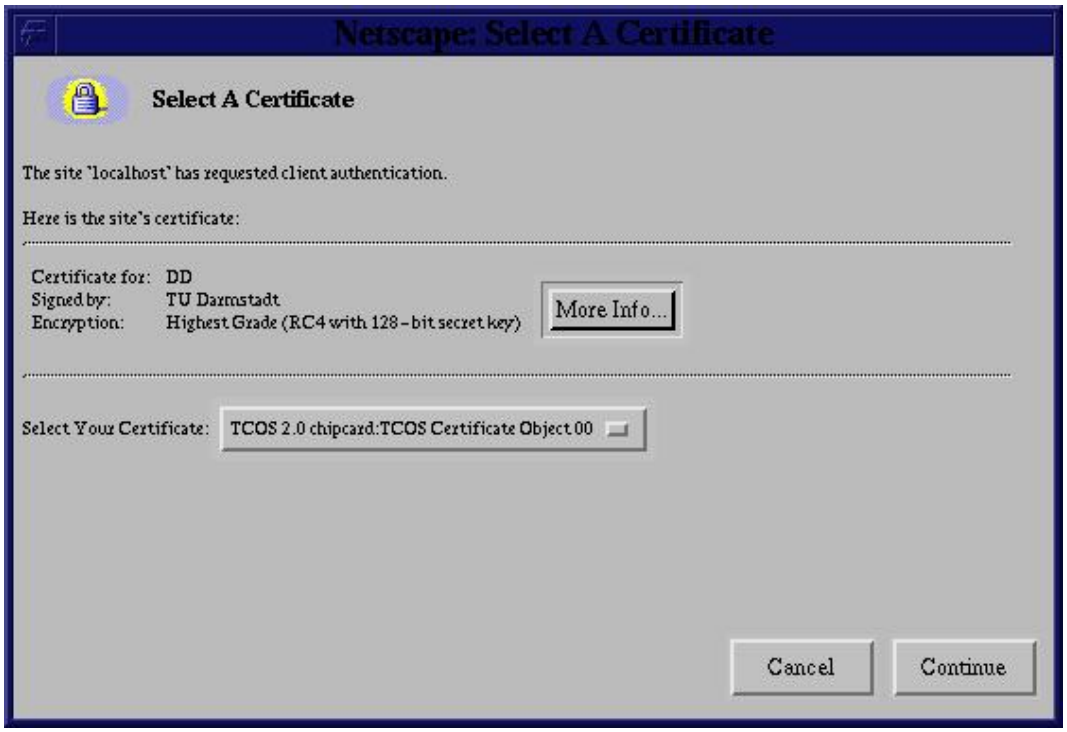

Figure 4.5: Selecting a Certificate

You can configure which default certificate to use by clicking **Security, Navigator** and choosing the desired certificate as **Certificate to identify you to a web site**.

Once the connection is establish, notice the padlock in the lower left-hand corner and in the middle of the tool bar. It should be in closed position, indicating that you are operating in secure mode. In insecure mode it would be opened, which would indicate that you are not using KOBIL Smart Token and not operating in secure mode.

Click **View, Page Info** to display the information regarding the server's certificate and the connection's encryption mode.

4.3 Secure E-mail Communication using Netscape Messenger

In this section, you'll learn how to secure your e-mails with Netscape Messenger using KOBIL Smart Token.

4.3.1 Choose your Certificate

To enable secure E-Mail, click on **Security, Messenger**(see figure 4.6). For some versions of Netscape, you need to choose the same global settings here that you also choose below, for the message specific options, for other version you might have to enable everything that you might want to enable in a mail.

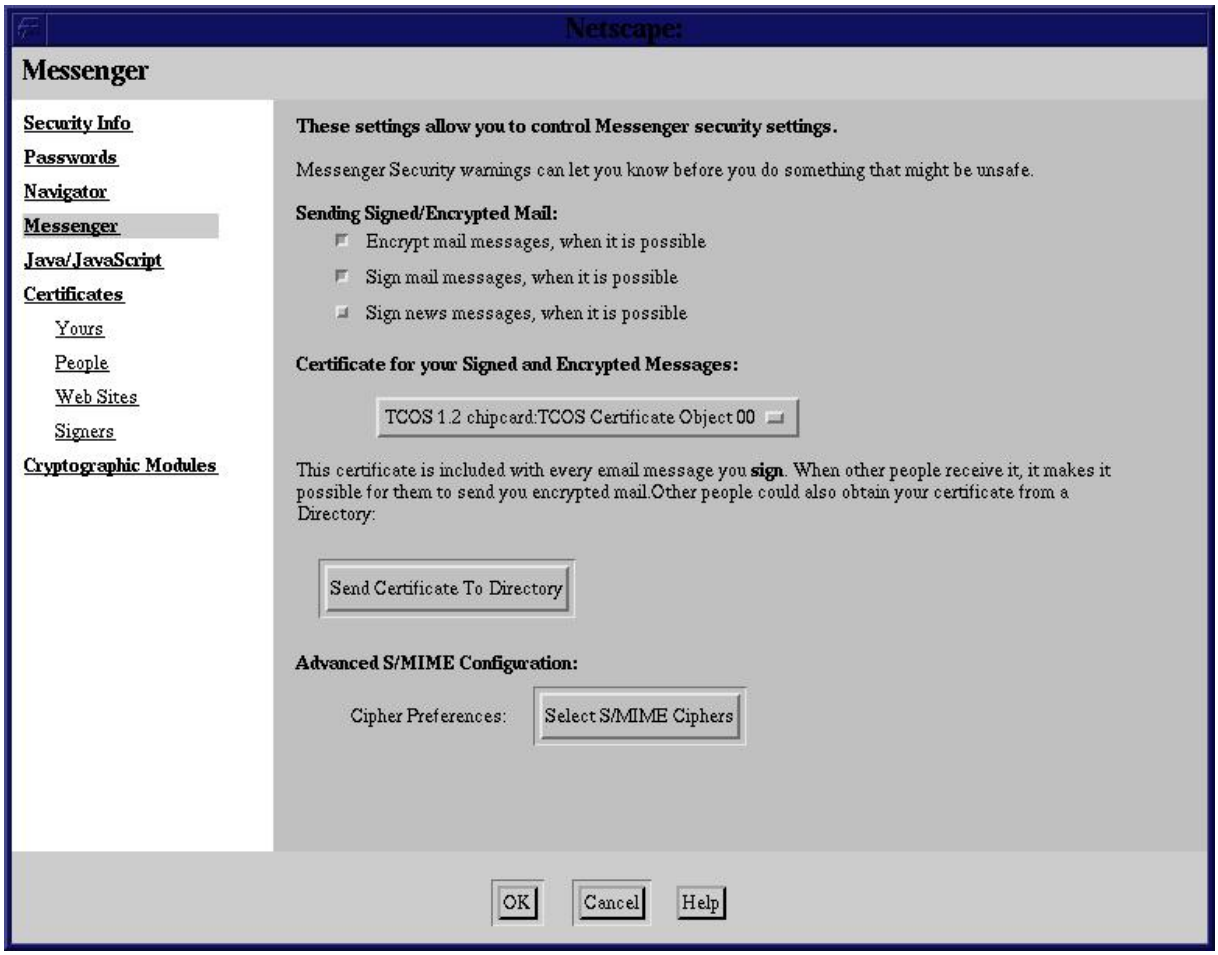
Netscape:
Messenger
Security Info
Passwords
Navigator
Messenger
Java/JavaScript
Certificates
Yours
People
Web Sites
Signers
Cryptographic Modules
These settings allow you to control Messenger security settings.
Messenger Security warnings can let you know before you do something that might be unsafe.
Sending Signed/Encrypted Mail:
Encrypt mail messages, when it is possible
Sign mail messages, when it is possible
Sign news messages, when it is possible
Certificate for your Signed and Encrypted Messages:
TCOS 1.2 chipcard:TCOS Certificate Object 00
This certificate is included with every email message you sign. When other people receive it, it makes it possible for them to send you encrypted mail.Other people could also obtain your certificate from a Directory:
Send Certificate To Directory
Advanced S/MIME Configuration:
Cipher Preferences:
Select S/MIME Ciphers
OK
Cancel
Help

Figure 4.6: Global Mail Options

Before you are ready to send an encrypted mail, you need to know the recipient's certificate (see above), if you want to send a message to several persons, you need to know a certificate for each of them, or your message will not be sent at all.

Once you receive a signed message from someone, the sender's certificate will be stored automatically, so you usually will not have to do this yourself. To view the list of certificates already known to your browser, click **Security, Certificates, People** (see figure 4.4). Your browser also automatically checks that the name in the e-mail address you are writing to corresponds to the name in the certificate.

In the same way, whenever you receive a signed message, your browser checks that the e-mail address of the sender matches his certificate.

In addition to globally setting/enabling security options you also can change this options in the mail header. If you click the icon for the sending options, the screen shown in figure 4.7 is displayed.

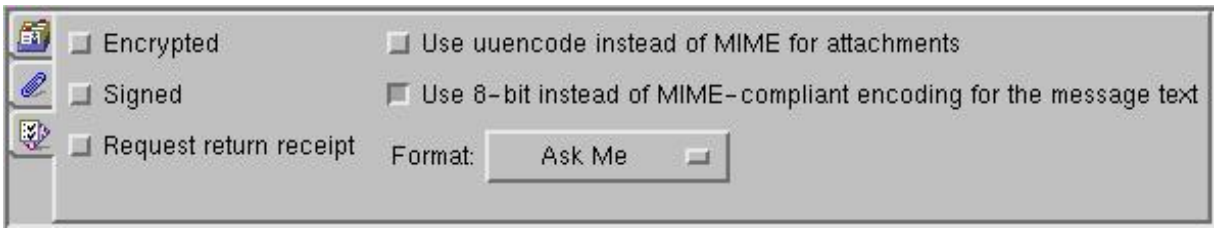

Figure 4.7: Sending Mail Options

Depending on the your Netscape version, make sure, that the options you choose here are the same as those that are globally set or that at least you do not enable a feature that is disabled in the global options. If Netscape does not like the options you did choose, it will complain that you do not have a certificate although you do have one. If this occurs, remember to change either the global or the sending options in such a way that they match each other.

4.3.2 Sending secure E-Mail

After having chosen your e-mail certificate, you can start securing your e-mails as follows:

1. You can send your message in plain text - just as before.
2. You can sign your message. This will include your signature and your certificate into the e-mail. As the certificate contains your public key, anybody now can verify that the mail was send by you. This provides authenticity and integrity.
3. You can encrypt a message with the recipients public key. Thus the message can be read by the recipient only, as he is the only one able to decrypt your message. This provides confidentiality.
4. You can combine both encryption and signature to get confidentiality and authenticity and integrity.

4.3.3 Receiving secure E-Mail

If you receive a secured e-mail, Netscape shows a symbol representing the e-mail's status:

- **Signed:**This e-mail was signed and the signature was successfully verified. Click on the **Signed** image to look at details such as the signer's certificate.
- **Invalid Signature:** This e-mail was signed, but the signature was not successfully verified. Click on the **Invalid Signature** image to look at possible reasons why the verification failed.
- Enrypted:This e-mail was encrypted. Click on the **Encrypted** image to look at details such as the encryption algorithm.
- Invalid Encryption This e-mail was encrypted, but could not be decrypted. Click on the **Invalid Encryption** image to look at possible reasons why the decryption failed.
- Signed and Encrypted:This e-mail was signed and encrypted. Click on the **Signed and Encrypted** image to look at details such as the signer's certificate and encryption algorithm.

Appendix A

Problems and Solutions

In this chapter, typical problems using KOBIL Smart Token are identified and described. If you do not find the solution for your particular problem here, take a look in the web at **www.kobil.de** where you will find a FAQ list which is always kept up-to-date.

A.1 KOBIL Smart Token for Microsoft-Applications

- **Certificate enrollment fails:**
  - Make sure that your Certification Authority (CA) supports CSP's correctly.
- **Outlook refuses to send a signed mail:**
  - Make sure that you have already a certificate (see Section 2.3.1).
  - Make sure that your certificate is valid.
- **Outlook refuses to send an encrypted mail:**
  - Make sure that you have the recipient's certificate (see Section 2.1.4).
- **Outlook cannot decrypt a mail that has been sent to you:**
  - If the mail was not encrypted with your certificate, you cannot decrypt it.
  - If the mail was encrypted with a certificate that you have deleted on your card, you are not able to decrypt it.
- **Authentication to a secure Web site fails:**
  - The secure web server may not accept the Certification Authority (CA) where you enrolled your certificate.
  - Your certificate may be not be valid or revoked.
- **Windows 2000 smartcard logon doesn't work:**
  - Make sure that a PC/SC driver is installed for your chipcard terminal. Your KOBIL chipcard terminal must appear in the device manager under *Smart Card Readers*.
  - You need a special smartcard login certificate on your TCOS chipcard (see section 3.3). Other certificates will not work.
  - Windows 2000/XP smartcard login requires a Windows 2000 / .net Server acting as a domain controller.

- Just after installing the Windows 2000 CA, it can take some time until the new CA root certificate and the certificate revocation list are distributed to the clients. The Windows group policy interval is 8 hours by default. Check first, if you can logon at your server using your smartcard (it may be necessary to change the domain controller's local security policy to allow normal users to logon).

A.2 KOBIL Smart Token PKCS#11 module for Netscape

- **Netscape refuses to send a signed mail:**
  - Make sure that you have already a certificate (see Section 4.3).
  - Make sure that your certificate for signed and encrypted mails is correctly set (see Section 4.6).
  - Make sure that your certificate is valid. Chose your certificate as shown in figure 4.3 and click on the **Verify** button.
- **Netscape refuses to send an encrypted mail:**
  - Make sure that you have the recipient's certificate (see Section 4.1.2).
- **Netscape cannot decrypt a mail that has been sent to you:**
  - If the mail was not encrypted with your certificate, you cannot decrypt it.
  - If the mail was encrypted with a certificate that you have deleted on your card, you are not able to decrypt it.
  - If you are running an older version of Netscape, you might not have full encryption strength. In that case, you should use the latest Netscape version or install **Fortify** (see www.fortify.net).
- **Authentication to a secure Web site fails:**
  - The secure web server may not accept the Certification Authority (CA) where you enrolled your certificate.
  - Your certificate may be not be valid or revoked.
  - If you are running an older version of Netscape, you might not have full encryption strength. In that case, you should use the latest Netscape version or install **Fortify** (see www.fortify.net).

Appendix B

Cryptographic Basics and Standards

B.1 Security Objectives

Confidentiality Protection from disclosure to unauthorised persons who may try to listen to communication or to steal some information.

Integrity Maintaining data consistency. Nobody except the originator can change the information while it is stored somewhere or transfered in an insecure media like the Internet.

Authentication (Non-repudiation / Access control) Assurance of identity of a person or an originator of data. The originator of some data cant deny it later. Unauthorized persons are kept out.

B.2 Terms and Basics

Cryptography is the science of keeping information secure. Cryptographic systems usually consist of two implemented processes: encryption and decryption.

Encryption is the process of transforming a message (the plaintext) into another message (the ciphertext) such that it is computationally infeasible to derive the plaintext data by reversing the process without knowledge of secret parameters. Many cryptographic algorithms mathematically combine input plaintext data and an encryption key to generate ciphertext data.

Decryption is the reverse process of encryption and transforms the ciphertext data back into the original plaintext data by using a complex function and a decryption key. One of the goals of cryptography is to raise the cost of guessing the decryption key beyond what is practical. The algorithm type and the key length are the most important measures against predictability of the key.

Cryptography has nothing to do with obscurity. Cryptographic algorithms and protocols should be conform with standards to support interoperability. Using non-published algorithms is contraproductive to compatibility. Moreover, cryptography is not about hiding algorithms, but it is about designing strong algorithms and secure mechanisms. Security and interoperability must both be achieved in years by building and testing very well-known algorithms, mechanisms and protocols. Security should be obtained only by storing the keys in a secure way and by making algorithms so strong that they are impractical to break.

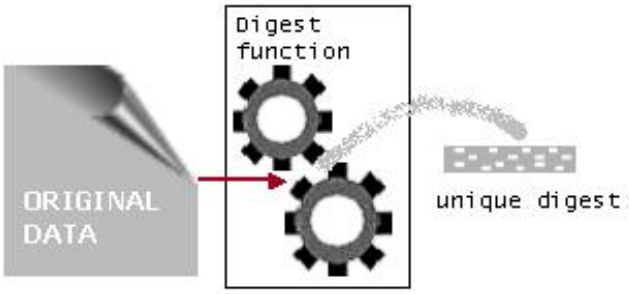

Figure B.1: Data Digest scheme

B.3 Standards

B.3.1 Data Digestion Algorithms

Data Digestion Algorithms are not used for encryption or decryption. The main purpose of these algorithms is to produce a unique "fingerprint" (typically 16 or 20 bytes in length) of the original data.

Digestion algorithms are also called "one-way hash functions", because it is computationally infeasible to recover the original data from its digest or even to find some other data which will produce the same digest. Ideally, each digest is unique and every bit is influenced by every bit of its input data. These algorithms are used together with other types of algorithms to supply digital signature processes (see below). The most common digestion algorithms are MD5, RipeMD and SHA1. Figure B.1 illustrates the data digestion process.

B.3.2 Symmetric Encryption Algorithms

With these type of algorithms, the same key (the so-called "session key") is used to encrypt and the decrypt the message. They are also known as "session key algorithms". Figure B.2 illustrates the symmetric encryption process.

The main advantage of symmetric algorithms is their speed of data encryption and decryption. The main weakness is the key management. Both sender and receiver must have the same secret session key which must be transferred securely. It is convenient and secure to transfer session keys by using public key algorithms. The most common session key algorithms currently are triple DES, RC2 and RC4.

B.3.3 Public Key Algorithms

Properties

With these algorithms, encryption and decryption keys are different. Each user has at least one key pair consisting of two keys. One is kept secret, so it is called a "private key", and the other one is open, which is called "public key". Private keys are unique for each user and they are never transferred to other people.

If someone needs to send a data to you, he needs your public key. He encrypts data with your public key and no one except you can decrypt the scrambled data using your private key. The transfer (or distribution) of your public key is secured by the help of "trusted authorities". Such a trusted authority will provide you a certificate for your public key. This means that they provide a packet of data containing both your public key and the trusted authority's assurance that this is really your public key. Figure B.3 illustrates the usage of public key process for a secure data transfer.

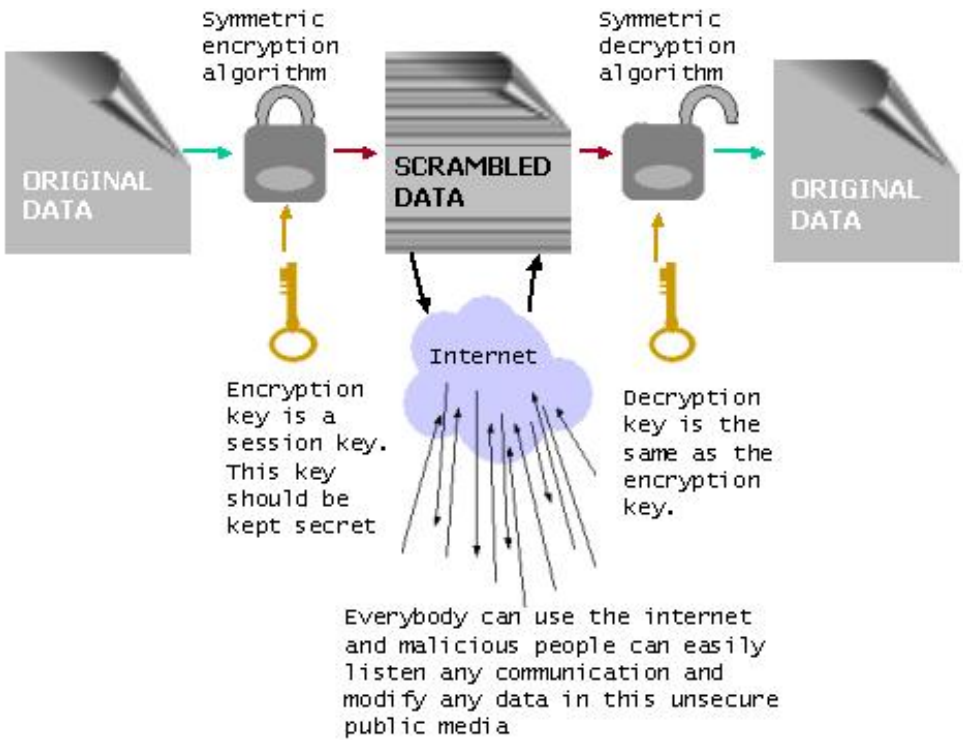

Figure B.2: Symmetric Algorithm

The main advantage of the public key algorithms is the secure key distribution. Their main disadvantage is the slow processing speed for encryption and decryption of large data. Because of this slowness, public key algorithms are used with together with symmetric session key algorithms to supply the necessary speed. To support confidentiality, public key algorithms are used to wrap and unwrap the session keys (for a secure session key transfer). To support both integrity and authentication, public key algorithms are used to sign and verify the output of data digestion algorithms. The most common public key algorithm is RSA.

Wrap Session Key

Bulk data is encrypted with a session key to supply fast speed. The encryption session key must be sent to the recipient for decryption. For a secure transfer, the session key is encrypted with the public key of the recipient. No one except the recipient can recover the session key, because the private key of the recipient is needed to decrypt the scrambled session key. Encrypted bulk data and the scrambled session key are merged to form a digital envelope. Someone who wants to recover the original data must recover the session key first (see figure B.4).

Unwrap Session Key

The recipient of the digital envelope detaches the scrambled session key from the encrypted bulk data. First, the scrambled session key is decrypted with the private key of the recipient. Second, bulk data is decrypted with the recovered session (decryption) key as shown in figure B.5.

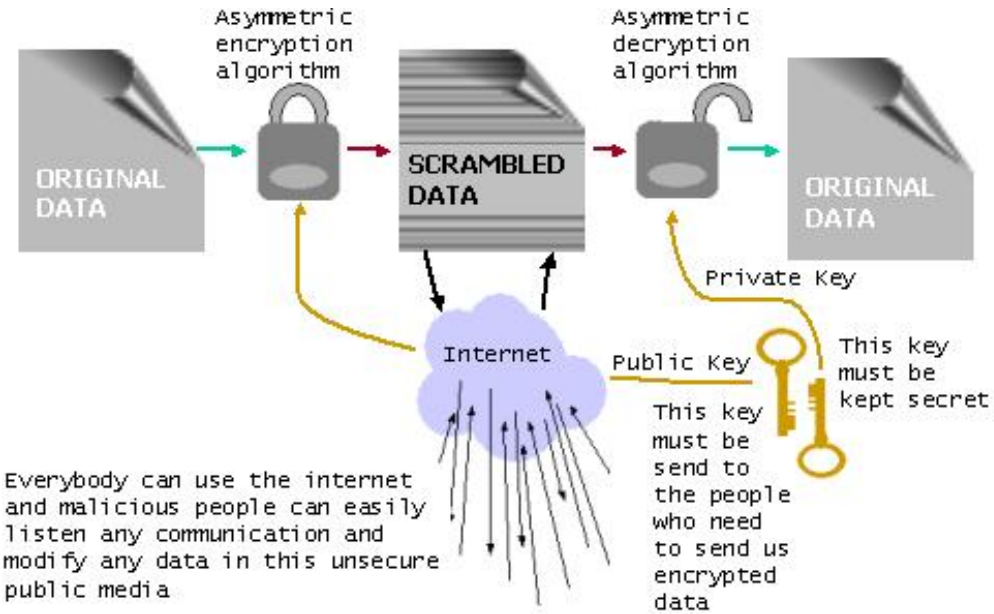

Figure B.3: Asymmetric Algorithm

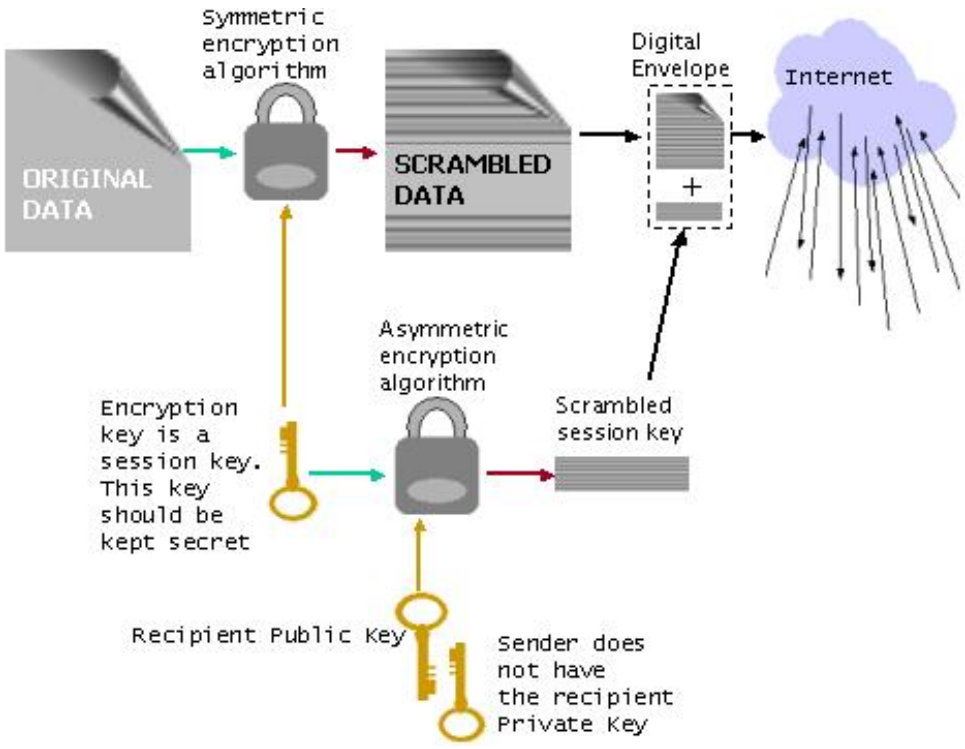

Figure B.4: Wrap Session Key

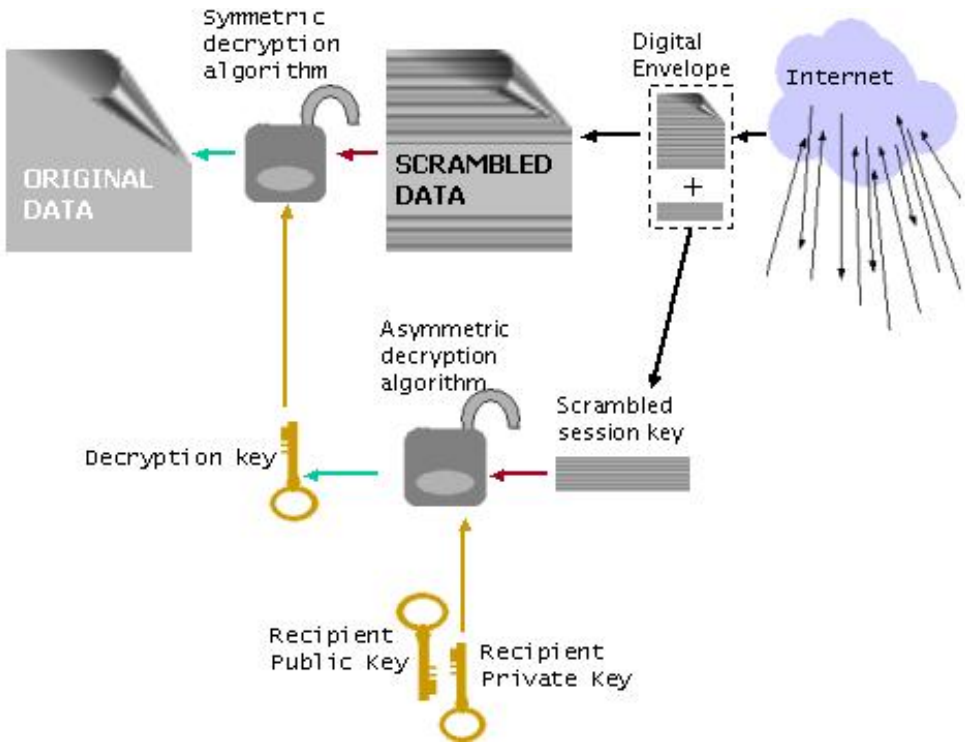

Figure B.5: Unwrap Session Key

Digital Signatures

Digital signatures are needed for the authentication of identities. A digital signature binds an individual to unique data. That's why there are two inputs of the signing process: first, the data itself and second, the private key of the signing individual.

Digestion algorithms are used to reduce the size of the bulk data because of the slowness of the public key algorithms. First, the message is digested and then the unique digest is encrypted with the originator's private key. Output is the signature. Anybody can decrypt this signature, because anybody can get the corresponding public key of the sender. The result of decryption is the unique digest and it is practically infeasible to find another message with the same digest.

Verification of Digital Signatures

To verify a digital signature, someone needs both the signature and the input data. A recipient of the signature decrypts it with the sender's public key to recover the data digest. The recipient also digests the input data to get the original data digest. If the recovered data digest is the same as the original digest, the signature is correct. Otherwise, the sender is not the person who he claims to be or the original data was modified on its way. Digital signatures support both authentication and integrity. For confidentiality, digital signing process is combined with the encryption process of session keys and the wrap operation of public keys.

B.3.4 Digital Certificates

A certificate is a set of data that includes a public key and other owner- specific information to identify an entity. The certificate owner has the corresponding private key. Certificates are issued by certification authorities (CA) which are

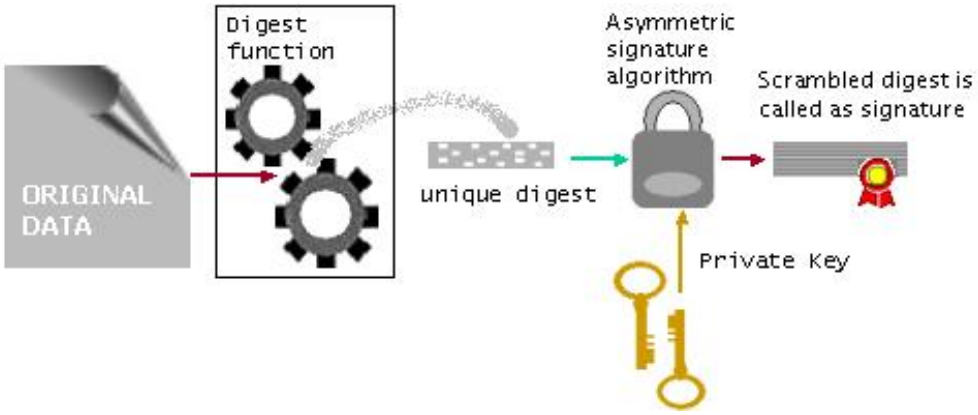

Figure B.6: Signature Creation

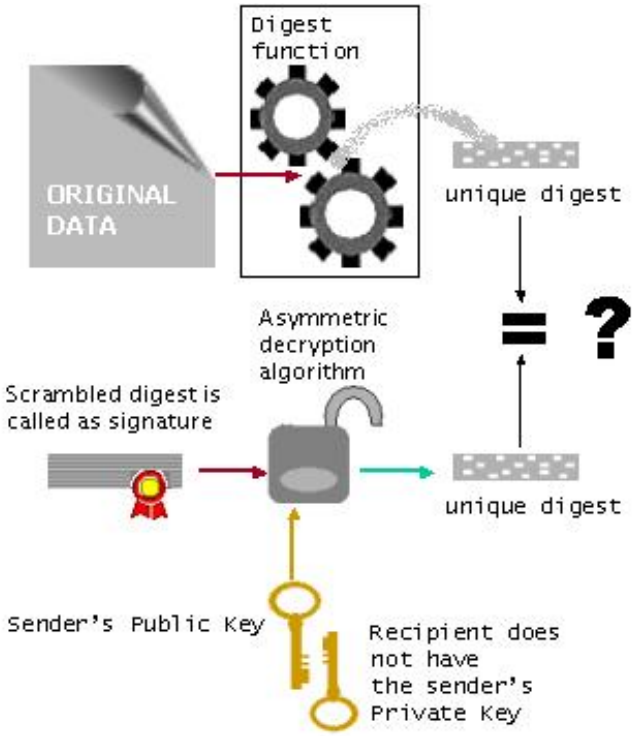

Figure B.7: Signature Verification

trusted organisations. Each certificate is protected by a signature that is created by a CA. Certification authorities and certificates make public key distribution secure. Secure storage and usage of a certificate and its corresponding private key is the problem of its owner. KOBIL Smart Key helps certificate owners with this problem by presenting a hardware based security system that uses smart cards.

The most widely accepted standard for digital certificates is defined by International Telecommunications Union's ITU-T X.509 standard. A X.509v3 certificate includes the following data fields:

- Version
- Certificate's serial number
- Signature algorithm ID
- Issuer name
- Expiration date
- User name
- User public key information
- Issuer unique identifier (optional)
- User unique identifier (optional)
- Extensions (optional, contain certificate usage instructions)
- Issuer's signature over the fields above

B.3.5 Certificate Authorities

A certificate authority (CA), also called "trust center", is a trusted organisation that issues public key certificates. A CA acts as a guarantor of the binding between the subject's public key and the subject's identity information that is contained in the certificates it issues.

The typical process of getting and using a certificate goes something like this (the user is called *Alice*[1] in this example):

1. Alice creates a cryptographic key pair, consisting of a private and a public key.
2. Alice creates a certificate request that contains her name, her public key, and perhaps some additional information.
3. Alice signs her certificate request with her new (corresponding) private key.
4. Alice sends the signed request to a CA.
5. The CA creates a data set from Alice's request.
6. The CA signs the data set with its private key.
7. The CA forms a certificate with the data set and its signature.
8. The CA returns the certificate to Alice who is now the owner of the certificate.

[1] In cryptographic protocols, the users are often called *Alice* and *Bob*

To give a real meaning to this process, the CA would of course need to make sure that Alice really is Alice (and not e.g. Bob claiming to be Alice). This however causes additional costs and actions in real life, so this is something which a pure Internet service cannot provide. However, there are companies offering that type of service.

Today's most popular browsers and e-mail programs know the certificates of very well known and more or less trusted CAs. So people can easily verify the signatures of many CAs. This helps people to decide whether a certificate and its content is trustworthy or not. If a certificate is signed and issued by an unknown CA and your browser does not have the public key of that CA, then your browser gives a warning and asks whether to proceed or not.

The typical certificate distribution and verification between users:

1. Alice sends her certificate to Bob to give him access to her public key. This is typically achieved by sending a signed, but not encrypted, message to Bob.
2. Bob verifies the signature of Alice's certificate by using the CA's public key. If the signature proves to be valid, he accepts the public key in the certificate as Alice's public key. Today's browsers and e-mail programs handle verification automatically.

B.3.6 Smart Cards and Readers

Smart cards are credit card-sized devices with integrated circuit chips (ICC) on them. They have their own security mechanisms to lock themselves against physical, electrical and chemical attacks. When private keys are loaded, they never leave the smart card and a PIN code protects the key usage. Smart Cards are easy to use. They can fit in a wallet and can be easily carried.

Terminals (often called readers, although they are usually able to write as well) are the devices which enable communication between a smart card and a computer. Smart card terminals can be connected to computers via serial or USB ports. An important advantage of some (more expensive) terminals is the secure PIN entry option, which is possible if a reader has its own keypad, display and special software on it.

B.3.7 Secure Socket Layer(SSL)

Secure Sockets Layer (SSL), developed by Netscape Communications, is a standard security protocol that provides security and privacy on the web. The protocol allows client/server applications to communicate securely. This is achieved by an online, interactive process which handles secure and authentic exchanges of some random data which is finally used to generate the session key on both sides. SSL uses both public key and session key algorithms. Work flow of the SSL is illustrated in figure B.9. In many cases, client authentication is optional, since clients may not have certificates.

B.3.8 Secure Multipurpose Internet Mail Exchange (S/MIME)

Secure Multipurpose Internet Mail Extensions (S/MIME) is an open protocol standard developed by the RSA Laboratories that provides encryption and digital signature functionality to Internet e-mail. S/MIME uses public key cryptography standards to define e-mail security services. S/MIME includes offline processes.

The sender's process is illustrated in figure B.10, the recipient's process is illustrated in figure B.11.

Figure B.8: Smart Card Terminals

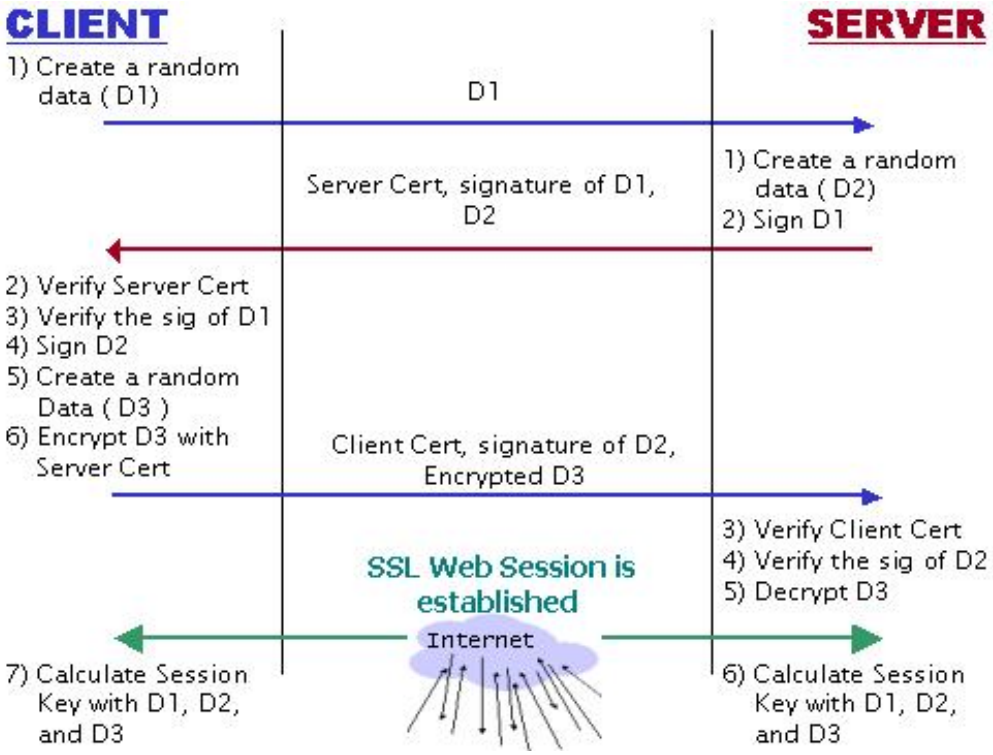
CLIENT
SERVER
1) Create a random data (D1)
D1
1) Create a random data (D2)
2) Sign D1
Server Cert, signature of D1, D2
2) Verify Server Cert
3) Verify the sig of D1
4) Sign D2
5) Create a random Data (D3)
6) Encrypt D3 with Server Cert
Client Cert, signature of D2, Encrypted D3
3) Verify Client Cert
4) Verify the sig of D2
5) Decrypt D3
SSL Web Session is established
Internet
7) Calculate Session Key with D1, D2, and D3
6) Calculate Session Key with D1, D2, and D3

Figure B.9: Secure Socket Layer

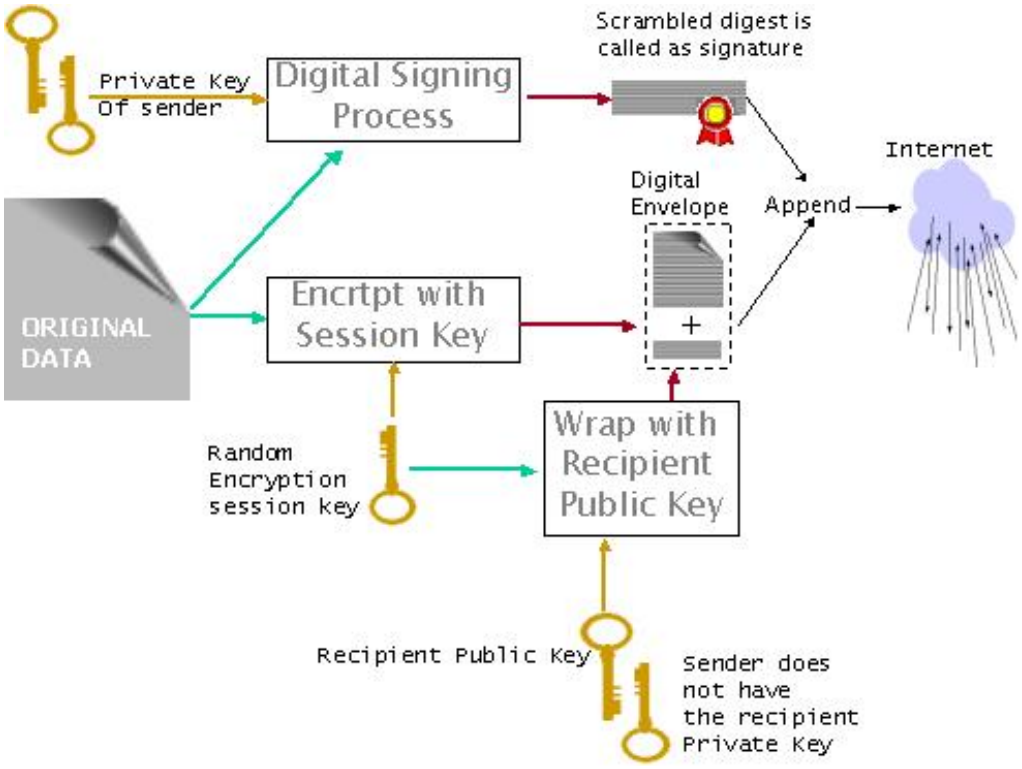

Figure B.10: Sender Process in S/MIME

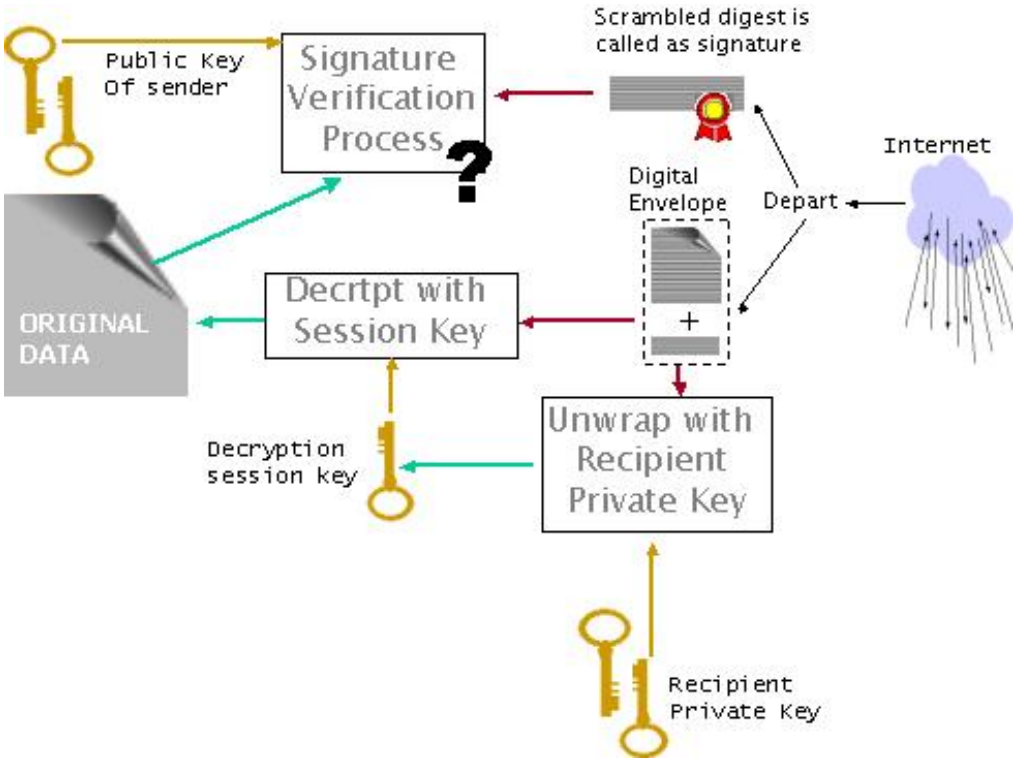

Figure B.11: Recipient Process in S/MIME

Appendix C

Glossary

Algorithm A mathematical formula used to perform computations that can be used for security purposes.

Authenticate To determine the identity of the entity that signed a message (entity authentication), or to verify that a message was not altered (data authentication).

Certificate Authority (CA) An entity with the authority and methods to certify the identity of one or more parties in an exchange (an essential function in public key crypto systems).

Cryptography The art and science of transforming confidential information to make it unreadable to unauthorised parties.

Data Encryption Standard (DES) A block cipher that encrypts data in 64-bit blocks. DES is a symmetric algorithm that uses the same algorithm and key for encryption and decryption. Developed in the early 1970s, DES is also known as the DEA (Data Encryption Algorithm) by ANSI and the DEA-1 by ISO.

Decryption The process in which ciphertext is converted to plaintext.

Digital Certificate A digital certificate provides identification for secure transactions. It consists of a public key and other data about the user, all of which is digitally signed by a Certificate Authority. It is a condition of access to secure e-mail or to secure Web sites.

Digital Signature A data string produced using a public key crypto system to prove the identity of the sender and the integrity of the message.

Encryption A cryptographic procedure whereby a legible message is encrypted and made illegible to all but the holder of the appropriate cryptographic key.

Internet Explorer (IE) Microsoft Internet browser.

Inter-operability The ability of products manufactured by different companies to operate correctly with one another.

Key A value that is used with a cryptographic algorithm to encrypt, decrypt, or sign data. Secret key (symmetric) crypto systems use only one secret key. Public key (asymmetric) crypto systems rely on a matched key pair to encrypt and decrypt data.

Key Length The number of bits forming a key. The longer the key, the more secure the encryption.

MD5 A hashing algorithm that creates a 128-bit hash value, which is twice the size of the block (64 bits).

Personal Computer/Smart Card (PC/SC) Standards that define the interface between smart cards and smart card readers.

Public Key Cryptography Standards (PKCS) A cryptographic system that uses two different keys (public and private) for encrypting data. The most well-known public key algorithm is RSA.

Rivest, Shamir, Adleman (RSA) Developers of the RSA public key crypto system and founders of RSA Data Security, Inc.

Secure Hash Standard (SHA) A standard designed by NIST and NSA. This standard defines the Secure Hash Algorithm (SHA-1) for use with the Digital Signature Standard (DSS).

Secure Sockets Layer (SSL) Security protocol used between servers and browsers for secure Web sessions.

SSL Handshake The SSL handshake, which takes place each time you start a secure Web session, identifies the server. This is automatically performed by your browser.

Secure/Multipurpose Internet Mail Extensions (S/MIME) Standard offline message format for use in secure e-mail applications.

Uniform Resource Locator (URL) Web address.